POLITIQUE DE CERTIFICATION et DECLARATION PUBLIQUE DES PRATIQUES DE CERTIFICATION

CERTINOMIS WEB ROOT CA
CERTINOMIS AC WEB G2
CERTINOMIS AC SAFE G2

EMETTEUR	DESTINATAIRES	COPIES
CERTINOMIS	PUBLIC	

Certinomis

Docaposte Certinomis SAS au capital de 40 156 euros.

Siège social : 45-47, Boulevard Paul Vaillant-Couturier

94200 Ivry sur Seine – France. RCS Créteil B 433 998 903

Historique des versions

DATE	VERSION	EVOLUTION	AUTEUR
05/12/2024	1.0	Version initiale	CERTINOMIS
24/12/2024	1.1	Version corrigée suite à l'audit de qualification	CERTINOMIS
05/03/2025	1.2	Mise à jour de la durée de conservation des archives au chapitre 5.5.2.3	CERTINOMIS

Table des matières

AVERTISSEMENT

1 INTRODUCTION

1.1 PRESENTATION GENERALE

1.1.1 IGC Certinomis

Certinomis est un Prestataire de Service de Certification Electronique (PSCE) dont le métier est la garantie de l'identité au sens large dans les échanges électroniques : identité des personnes physiques agissant pour leur compte propre ou au nom d'une personne morale, ou identification d'une personne morale responsable de la mise en œuvre d'une application informatique.

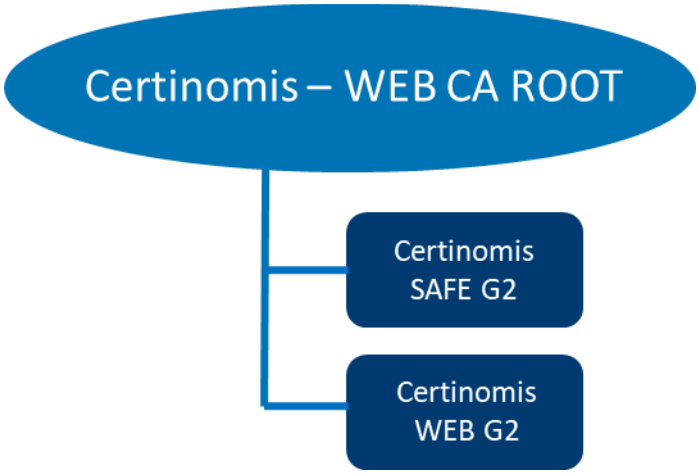
Le PSCE réalise ses missions en émettant des certificats électroniques au travers de différentes Autorités de Certification (AC) qui s'insèrent dans une Infrastructure à Clé Publique (IGC), un ensemble de moyens techniques, humains, documentaires et contractuels mis à la disposition d'utilisateurs pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques.

La mise en place d'une IGC, nécessaire à la sécurité et à la confiance, ouvre une palette de services à valeur ajoutée pour les transactions électroniques (par exemple : transactions commerciales, signature de contrats, téléprocédures, etc.).

Ils ont pour fonction d'assurer :

- l'intégrité des messages ;
- l'identification et l'authentification[1] ;
- l'authenticité de l'origine ;
- et la confidentialité.

L'IGC publique de Certinomis est composée de deux Autorités de Certification Racine. La présente PC concerne l'AC Racine « CERTINOMIS WEB ROOT CA » et ses deux AC intermédiaires. Cette hiérarchie est dédiée au service d'émission de certificats pour l'authentification de serveurs.



1.1.2 Objet du document

La présente Politique de Certification et Déclaration publique des Pratiques de Certifications a pour objet de permettre l'émission de certificats identifiant des applications informatiques et la personne morale responsable de leur mise en œuvre, et qui seront utilisés pour l'authentification des applications qu'ils identifient ou pour protéger la confidentialité des échanges.

Elle concerne l'AC Racine « CERTINOMIS WEB ROOT CA » et ses deux AC intermédiaires.

[1] Étant précisé que ce n'est pas au sens des actes authentiques, tels qu'ils sont régis par les articles 1317 et suivants du code civil, mais au sens technique d'authentification cryptographique

La présente Politique de Certification et Déclaration publique des Pratiques de Certifications détaille comme son nom l'indique, certaines pratiques de certifications au public de sorte à se conformer aux exigences exprimées par le Cab Forum en la matière.

La Politique de Certification et Déclaration publique des Pratiques de Certifications définie dans le présent document est destinée à être utilisée par les entreprises, les associations, les ministères, les entités administratives ou gouvernementales et groupements de toute sorte, ainsi que les individus. Les personnes qui consultent et utilisent ce document peuvent s'informer auprès de l'AC émettrice afin d'obtenir plus de détails sur sa mise en œuvre.

La Politique de Certification et Déclaration publique des Pratiques de Certifications couvre la gestion et l'utilisation de certificats, selon leurs classes, contenant les clés publiques servant aux fonctions de vérification, d'authentification, d'intégrité et de concordance des clés.

La Politique de Certification et Déclaration publique des Pratiques de Certifications couvre aussi la gestion et l'utilisation de certificats contenant les clés publiques servant aux fonctions de confidentialité. Les certificats délivrés en vertu de la présente politique permettent d'assurer le secret d'informations, considérées comme privées ou sensibles par leur propriétaire. Les certificats ne servent pas à protéger les renseignements classifiés.
La délivrance d'un certificat de clé publique en vertu de la présente politique ne signifie pas que le client ou le bénéficiaire soit autorisé de quelque façon que ce soit à faire des transactions commerciales, ou autres, au nom de l'organisation qui exploite l'AC.
L'AC sera assujettie aux lois et règlements en vigueur sur le territoire de la République française, ainsi qu'aux normes européennes en vigueur et aux conventions internationales ratifiées par la France, et qui touchent à l'application, l'élaboration, l'interprétation et la validité des politiques de certification mentionnées dans le présent document.

L'AC se réserve le droit de ne pas conclure d'accord de certification croisée avec une autorité de certification externe.

1.2 IDENTIFICATION DU DOCUMENT

La désignation du numéro d'identification d'objet (OID) du présent document est : 1.2.250.1.86.2.6.0.100.1
Ce document couvre plusieurs politiques de certifications, pour chacune desquelles un OID a été attribué. La politique ETSI adoptée comme base est précisée dans le tableau ci-dessous pour chaque PC Certinomis.

AC Racine : 1.2.250.1.86.2.6.0.100.1		
AC SAFE G2		
OID	*Usage*	*Conformité ETSI / RGS*
1.2.250.1.86.2.6.8.63.1	Authentification client et serveur	EN 319 411-2 QEVCP-w (0.4.0.194112.1.4)
1.2.250.1.86.2.6.8.62.1	Authentification client et serveur	EN 319 411-2 QNCP-w (0.4.0.194112.1.5)
AC WEB G2		
OID	*Usage*	*Conformité ETSI / RGS*
1.2.250.1.86.2.6.7.20.1	Authentification serveur	RGS 1 étoile, EN 319 411-1 OVCP (0.4.0.2042.1.7)
1.2.250.1.86.2.6.7.61.1	Authentification client et serveur	EN 319 411-1 OVCP (0.4.0.2042.1.7)
1.2.250.1.86.2.6.7.60.1	Authentification client et serveur	EN 319 411-1 DVCP (0.4.0.2042.1.6)

1.3 ENTITES INTERVENANT DANS L'IGC

Lorsqu'un prestataire fournit des services de certification, à savoir qu'il délivre des certificats ou qu'il fournit d'autres services liés aux signatures numériques, il convient de distinguer plusieurs métiers ou fonctions, desquels découlent des rôles et des responsabilités distincts.

Le processus de certification et la gestion du cycle de vie du certificat font appel à une grande diversité d'intervenants dans la chaîne de la confiance :

- Autorité de certification,
- Autorité d'enregistrement,
- Bénéficiaires de l'Autorité de Certification (Responsable du certificat),
- Sujet du certificat délivré par l'Autorité de Certification,
- Tiers utilisateurs.

1.3.1 Autorités de certification

L'Autorité de Certification est responsable vis-à-vis de ses clients, mais aussi de toute personne se fiant à un certificat qu'elle a émis, de l'ensemble du processus de certification, et donc de la validité des certificats qu'elle émet. A ce titre, elle édicte la Politique de Certification et valide les Déclarations de Pratique de Certification respectées par les différentes composantes de l'Infrastructure à Clé Publique.

La garantie apportée par l 'Autorité de Certification vient de la qualité des techniques mises en œuvre, mais aussi du cadre réglementaire et contractuel qu'elle définit et s'engage à respecter.

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation, ...) et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (IGC).

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats (cf. ci-dessous).

Autorité d'enregistrement (AE) - Cette fonction vérifie les informations d'identification du futur sujet d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC (cf. ci-dessous). L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du sujet du certificat lors du renouvellement du certificat de celui-ci.

Fonction de génération des certificats - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du sujet provenant soit du bénéficiaire, soit de la fonction de génération des éléments secrets du bénéficiaire, si c'est cette dernière qui génère la bi-clé du certificat.

Fonction de génération des éléments secrets du bénéficiaire - Cette fonction génère les éléments secrets à destination du bénéficiaire, et les prépare en vue de leur remise au bénéficiaire (par exemple, personnalisation de la carte à puce destinée au porteur, courrier sécurisé avec le code d'activation, etc.). Ces éléments secrets sont directement la bi-clé du certificat, les codes (activation / déblocage) sont liés au dispositif de stockage de la clé privée du bénéficiaire.

Fonction de remise au bénéficiaire- Cette fonction remet au bénéficiaire au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif cryptographique, clé privée du porteur, codes d'activation,...).

Fonction de publication - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux bénéficiaires et/ou aux utilisateurs de certificats, hors informations d'état des certificats. L'AC ne met pas à disposition les certificats valides de ses bénéficiaires.

Fonction de gestion des révocations - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction d'information sur l'état des certificats - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers : LCR, LAR.

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

Porteur - La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.

Responsable du certificat (RC) - Personne en charge et responsable du certificat électronique de service applicatif de cachet ou d'authentification du serveur.

Mandataire de certification (MC) - Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des bénéficiaires de cette entité (il assure notamment le face-à-face pour l'identification des bénéficiaires lorsque celui-ci est requis).

Utilisateur de certificat - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du bénéficiaire du certificat.

Personne autorisée - Il s'agit d'une personne autre que le bénéficiaire et le mandataire de certification et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du bénéficiaire (demande de révocation, de renouvellement, ...). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du bénéficiaire ou d'un responsable des ressources humaines.

1.3.2 Autorité d'enregistrement

L'Autorité d'Enregistrement applique des procédures d'identification des personnes physiques ou morales, conformément aux règles définies par l'Autorité de Certification. Son but est d'établir que le demandeur a bien l'identité et les qualités qui seront indiquées dans le certificat. Ces procédures d'identification sont variables selon le niveau de confiance que l'on entend apporter à cette vérification.

L'Autorité d'Enregistrement est le lien entre l'Autorité de Certification et le bénéficiaire. Qu'elle soit ou non directement en contact physique avec le bénéficiaire, elle reste dépositaire de ses informations personnelles.

Sa responsabilité ne peut être engagée que par l'Autorité de Certification. L'Autorité de Certification a un devoir de contrôle et d'audit des Autorités d'Enregistrement.

L'AE a pour rôle de vérifier l'identité du futur sujet du certificat. Pour cela, l'AE assure les tâches suivantes :

- la prise en compte et la vérification des informations du futur sujet et le cas échéant de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- le cas échéant, la prise en compte et la vérification des informations du futur MC et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- le cas échéant, la prise en compte et la vérification des informations du futur RC et du serveur informatique, ainsi que de leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- l'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC suivant l'organisation de cette dernière et les prestations offertes ;
- l'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du bénéficiaire ou, le cas échéant, du MC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

Seule l'AE Certinomis à la capacité de valider un nom de domaine internet (FQDN) en vue de l'émission d'un certificat serveur SSL/TLS reconnu publiquement dans le programme d'autorité racine des éditeurs de navigateurs internet

(notamment ceux membres du CAB Forum http://www.cabforum.org/forum.html). Cette fonction de validation ne peut en aucun cas être déléguée à un tiers. Cette fonction est assurée par le rôle de confiance spécialiste validation.

1.3.3 Responsable du certificat

Dans le cadre de la présente PC, un RC est une personne physique qui est responsable de l'utilisation du certificat du serveur informatique identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat. Le RC a un lien contractuel / hiérarchique / réglementaire avec cette entité.

Le RC respecte les conditions qui lui incombent définies dans la présente PC.

À noter que le certificat étant attaché au serveur informatique et non au RC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RC de l'entité, changement d'affectation et de responsabilité au sein de l'entité, etc.

L'entité doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RC de ses fonctions et lui désigner un successeur. Une AC révoquera un certificat serveur pour lequel il n'y a plus de RC explicitement identifié.

1.3.4 Utilisateurs de certificats

L'utilisateur du certificat peut être ;

- Une entité ou une personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du bénéficiaire du certificat.
- Un serveur sous la responsabilité d'une personne physique ou morale, qui utilise un certificat et un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le porteur du certificat. L'application met en œuvre la politique et les pratiques de sécurité édictées par le responsable d'application.

Avant d'accorder sa confiance au dit certificat, le tiers utilisateur doit impérativement vérifier sa validité auprès de Certinomis en consultant les Listes des Certificats Révoqués appropriées les plus récentes, ainsi qu'en vérifiant sa validité intrinsèque, en particulier sa date d'expiration et sa signature, et la validité de tout certificat sur l'itinéraire de confiance. A défaut de remplir cette obligation, le tiers utilisateur assume seul tous les risques de ses actions non conformes aux exigences de la présente politique, Certinomis ne garantissant, dès lors, plus aucune valeur juridique aux certificats qu'elle a émis et qui pourraient avoir été révoqués ou qui ne seraient pas valides.

1.3.5 Autres participants

1.3.5.1 Mandataire de certification

Le recours à un mandataire de certification (MC) n'est pas obligatoire pour une entité. Une même entité peut s'appuyer sur un ou plusieurs MC.

Dans le cas où elle y a recours, le MC doit être formellement désigné par un représentant légal de l'entité concernée. Le MC est en relation directe avec l'AE de l'IGC.

Le MC est une personne ayant, directement par la loi ou par délégation, le pouvoir d'autoriser une demande de certificat portant le nom de l'organisation. Il peut aussi avoir d'autres pouvoirs au nom de l'organisation, comme celui de révocation.

Dans le cadre d'une organisation, un MC peut être désigné pour effectuer les actes nécessaires à l'émission d'un certificat en lieu et place des clients.

Par défaut, le représentant légal de l'organisation est considéré comme MC.

Le MC doit :

- être une personne physique dûment autorisée à agir pour le compte d'une organisation ;

- effectuer correctement et de façon indépendante les contrôles d'identité des futurs porteurs de l'entité pour laquelle il est MC ;
- respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

Le MC peut désigner un opérateur de saisie. Cet opérateur est en charge de la saisie des données collectées au sein de l'organisation que le MC représente. Il s'engage – par contrat – à la plus stricte confidentialité pour les données dont il aura eu connaissance au cours de sa mission.

Le MC signe les données saisies par l'opérateur de saisie avant toute transmission auprès de l'Autorité d'Enregistrement.

L'entité doit signaler à l'AC, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigner un successeur.

1.4 USAGE DES CERTIFICATS

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats émis

Les certificats émis en vertu de la présente politique sont appropriés pour établir le lien qui existe entre une identité et une clé publique.

Certaines applications d'échanges dématérialisés peuvent nécessiter des certificats à des fins de tests ou de recette. Les mêmes exigences doivent être prises en compte pour de tels certificats, il n'y a pas de distinction entre de tels certificats et des certifications de « production ».

Authentification Serveur SSL
Usage du certificat serveur
Dispositif ou application qui utilise le certificat d'une entité identifiée afin d' • Établir une session sécurisée entre deux serveurs.

1.4.1.2 Bi-clés et certificats d'AC et de composantes

L'AC génère et signe différents types d'objets : certificats, LCR / LAR.

Pour signer ces objets, l'AC dispose d'une bi-clé.

L'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (hiérarchie d'AC).

Les bi-clés et certificats de l'AC sont utilisés pour la signature de certificats, de LCR / LAR et uniquement utilisés qu'à cette fin. Ils ne sont pas utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

1.4.2 Domaines d'utilisation interdits

Rien n'empêche techniquement la mise en œuvre d'applications considérées comme interdites au sens des critères énoncés ci-après. Toutefois, celui qui réaliserait ces opérations le ferait à ses seuls et entiers risques et périls, et serait tenu pour seul responsable des conséquences.

Si un bénéficiaire utilise ses certificats en dehors des applications appropriées, et en particulier dans une application interdite, telles que définies aux termes de la présente politique ou de la DPC, il le fait sous sa seule responsabilité et à ses entiers risques et périls.

Si le tiers utilisateur d'un certificat se fie à celui-ci alors que l'application est interdite ou restreinte aux termes de la présente politique ou de la DPC, il en assume seul tous les risques.

Les certificats émis par Certinomis ne peuvent, en aucune façon, être utilisés pour signer d'autres certificats (de personne ou d'organisation ainsi que de toute entité identifiée). La responsabilité civile et pénale de tout contrevenant pourra être engagée par Certinomis.

Dans aucune des hypothèses visées ci-dessus, la responsabilité de l'AC ne pourra être mise en jeu.

Personne n'est autorisé à utiliser la clé privée associée à un certificat pour signer un autre certificat ou une LCR en tant qu'AC.

1.5 GESTION DE LA PC

La présente politique s'applique aux AC et aux partenaires, à leur responsable, à leur personnel, aux certificats émis par les AC, aux Listes de Certificats Révoqués émises par les AC, aux clients et bénéficiaires des AC et aux tiers utilisateurs de certificats émis par les AC.
La présente politique est revue et mise à jour annuellement.

1.5.1 Entité gérant la PC

La présente politique de certification est sous la responsabilité de la société Certinomis.

1.5.2 Point de contact

Le directeur général de Certinomis
45-47, Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine

Téléphone : 0810 184 956
Courrier électronique : ld-politiquecertification@certinomis.fr

1.5.3 Entité déterminant la conformité d'une DPC internes avec cette PC

La Direction de Certinomis détermine la conformité de la DPC internes avec la présente politique de certification, soit directement soit indirectement en faisant appel à des experts indépendants spécialisés dans le domaine de la sécurité et des IGC.

La Direction de Certinomis a désigné parmi les collaborateurs de l'entreprise, un responsable de la conformité, en charge entre autres d'effectuer une veille régulière de l'évolution des exigences du Cab Forum (BRG et EVCG).

1.5.4 Procédures d'approbation de la conformité de la DPC internes

L'AC est garante de l'application de la DPC internes avec la Politique de Certification.
L'AC est responsable de la gestion (mise à jour, révisions) de la DPC internes. Toute demande de mise à jour de la DPC internes suit le processus d'approbation mis en place.
Une AGP peut demander l'examen de la DPC internes conformément aux procédures en vigueur.

1.6 DEFINITIONS ET ACRONYMES

1.6.1 Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

- AC Autorité de Certification
- AE Autorité d'Enregistrement
- AGP Autorité de Gestion des Politiques
- AH Autorité d'Horodatage
- DN Distinguished Name
- DPC Déclaration des Pratiques de Certification
- ETSI European Telecommunications Standards Institute
- IGC Infrastructure de Gestion de Clés.
- LAR Liste des certificats d'AC Révoqués
- LCR Liste des Certificats Révoqués
- MC Mandataire de Certification
- OID Object Identifier
- PC Politique de Certification
- PSCE Prestataire de Services de Certification Electronique
- RC Responsable du Certificat de service applicatif
- RSA Rivest Shamir Adelman
- SP Service de Publication
- SSI Sécurité des Systèmes d'Information
- URL Uniform Resource Locator

1.6.2 Définitions

Autorité de Certification (AC) :

Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre 1.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

Autorité d'enregistrement (AE) : Cf. chapitre 1.3.1.

Autorité de Gestion de la Politique (AGP) :

L'Autorité de Gestion de la Politique, pour les usages qui la concerne, établit les besoins et les exigences en termes de sécurité dans l'ensemble du processus de certification et d'utilisation des certificats. Elle établit des lignes directrices, qui peuvent prendre la forme d'un canevas de Politique de Certification, que doivent respecter toutes les Autorités de Certification qu'elle accrédite. Elle valide et suit toute évolution des politiques de certification des Autorités de Certification qu'elle accrédite.

Son rôle est celui d'une autorité morale qui indique par l'accréditation la confiance que l'on peut accorder à une Autorité de Certification.

Certificat :

Attestation électronique liant les données afférentes au chiffrement ou à la vérification de signature, des échanges, messages et documents électroniques à un sujet, afin d'en assurer la confidentialité ou d'en assurer l'authentification et l'intégrité.

Sujet :

Identités portées dans le certificat. Le sujet peut contenir l'identité d'une personne, d'un serveur, d'une organisation.

Bénéficiaire :

Personne physique identifiée par l'AE qui porte la responsabilité des certificats qui lui sont remis. Le bénéficiaire peut être le porteur ou le RC.

Porteur :

Personne physique possédant un certificat dont il en est le sujet. Le porteur est le bénéficiaire de son propre certificat.

Dispositif ou application (dit Serveur):

Matériel ou logiciel pouvant faire usage des certificats pour établir automatiquement un contexte de sécurité qui lui est propre. Par exemple, un serveur web, ou un routeur utilisant un certificat pour s'authentifier lors des échanges.

Politique de Certification (PC) :

Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les bénéficiaires et les utilisateurs de certificats.

Déclaration des Pratiques de Certification Internes (DPC internes) :

Une DPC internes identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Prestataire de services de certification électronique (PSCE) :

Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des bénéficiaires et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1 ENTITEES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

La fonction de publication de l'AC met à disposition l'information sur l'état des certificats par le biais de fichiers « LCR » et d'un répondeur OCSP.

Les points d'accès des LAR et des LCR sont précisés au chapitre 7 de la présente PC.

Le point d'accès du répondeur OCSP est précisé au chapitre 7 de la présente PC.

Les LCR et LAR sont aussi accessibles en téléchargement, directement sur le serveur WEB public : www.certinomis.fr dans la rubrique « Documents et liens / Nos listes de révocations ».

2.2 INFORMATIONS DEVANT ETRE PUBLIEES

L'AC a pour obligation de publier au minimum les informations suivantes à destination des RC et utilisateurs de certificats :

- sa politique de certification ;
- sa déclaration des pratiques de certification ;
- l'état des certificats émis par l'AC ;
- les certificats de l'AC en cours de validité ;
- si l'AC est rattachée à une hiérarchie d'AC, les certificats en cours de validité des AC de cette hiérarchie et les différentes politiques de certification correspondantes, ceci jusqu'à l'AC Racine ;
- pour les certificats d'AC autosignés (AC Racine), les informations permettant aux utilisateurs de certificats de s'assurer de l'origine de ces certificats (cf. chapitre VI.1.4) et de leur état (cf. chapitre IV.10) ;
- les formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, etc.).

La Politique de Certification, les certificats d'AC, les formulaires de demande de certificat, les contrats et conditions générales en vertu desquels les certificats sont émis, sont soit disponibles sur le site WEB de l'AC à l'adresse suivante http://www.certinomis.fr, soit communiqués dans le cadre de la négociation commerciale.
Une copie peut également être obtenue par courrier électronique.

Pour les clauses applicables sur les offres serveur TLS/SSL, Certinomis se conforme à la version courante des « Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates » (BR) publiée sur le site http://www.cabforum.org. En cas d'incohérence entre ce document et les exigences BR du CABForum, les exigences BR du CABForum sont applicables.

Pour les clauses applicables sur les offres serveur TSL/SSL EV, Certinomis se conforme à la version courante des " Guidelines for the Issuance and Management of Extended Validation Certificates " (EVCG) publiée sur le site http://www.cabforum.org. En cas d'incohérence entre ce document et les exigences EVCG du CABForum, les exigences EVCG du CABForum sont applicables

De plus, compte tenu de la complexité de lecture d'une PC pour des porteurs ou des utilisateurs de certificats non spécialistes du domaine, l'AC publie également des conditions générales d'utilisation sur son site web http://www.certinomis.fr dans la rubrique : « Documents et liens / Nos conditions générales d'utilisation ».

La Liste des Certificats Révoqués est fournie par l'AC qui en assure la publication sur son site public, dans la limite des éléments autorisés par ses clients et bénéficiaires.

2.3 DELAIS ET FREQUENCES DE PUBLICATION

Les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.) doivent être publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. En particulier, toute nouvelle version doit être communiquée au RC ou MC lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord. Les systèmes publiant ces informations doivent au moins être disponibles les jours ouvrés.

Les certificats d'AC doivent être diffusés préalablement à toute diffusion de certificats de services applicatifs et/ou de LCR correspondants et les systèmes les publiant doivent avoir une disponibilité 24h/24 et 7j/7.

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres IV.9 et IV.10.

Il est à noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information.

La Politique de Certification doit être mise à jour sur le site WEB du CCADB dans les 7 (sept) jours suivant sa mise à jour effective.

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un contrôle d'accès de type mots de passe longs basé sur une politique de gestion stricte des mots de passe.

3 IDENTIFICATION ET AUTHENTIFICATION

Le présent chapitre définit les exigences en matière d'enregistrement des demandes de certificats, c'est-à-dire, des clients, des bénéficiaires et des entités identifiées. Il définit également les exigences de vérification en matière de pouvoir, représentation et mandat.

3.1 NOMMAGE

3.1.1 Types de noms

Les noms utilisés doivent être conformes aux spécifications de la norme [X.500].

Dans chaque certificat conforme à la norme [X.509], l'AC émettrice (issuer) et le service applicatif d'authentification du serveur (subject) sont identifiés par un "Distinguished Name" (DN) répondant aux exigences de la norme [X.501].

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les services applicatifs dans les certificats doivent être explicites.

Le format du DN est précisé au chapitre 7.1.2.2 de la présente PC.

L'AC définit sa politique de nommage et, à ce titre, elle se réserve le droit de prendre toutes décisions concernant les noms des personnes, des organisations, qu'elles soient de droit public ou de droit privé, et de toutes autres entités identifiées dans le cadre des certificats signés. Une partie demandant un certificat doit être en mesure de prouver qu'elle a le droit d'utiliser un nom en particulier.

Une partie qui demande un certificat doit avoir le droit d'utiliser le nom qu'elle souhaite y voir figurer.

3.1.3 Pseudonymisation des identités

Les certificats objets de la présente PC ne peuvent en aucun cas être anonymes.

L'identifiant de l'entité dans son certificat ne peut être un pseudonyme.

3.1.4 Règles d'interprétation des différentes formes de nom

Sans objet.

3.1.5 Unicité des noms

Les noms distinctifs sont uniques pour toutes les entités identifiées d'une AC. Ainsi le DN des certificats de bénéficiaire contient un champ spécifique (serialNumber) composé de nombres séparés par un tiret afin de garantir le caractère unique du nom distinctif.

Pour les certificats DVCP, le champ serialNumber n'est pas présent.

3.1.6 Identification, authentification et rôle des marques déposées

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L. 711-1 et suivants du Code de la Propriété intellectuelle (codifié par la loi n°92-957 du 1er juillet 1992 et ses modifications ultérieures) appartient

au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

L'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par les clients et bénéficiaires des marques déposées, des marques notoires et des signes distinctifs, ainsi que les noms de domaine.

3.2 VALIDATION INITIALE DE L'IDENTITE

L'AE doit vérifier l'identification de l'organisation, de son représentant légal et de toutes personnes désignées par ce dernier, directement ou indirectement, pour le représenter vis-à-vis de l'AC ou de l'AE. Le représentant légal et ces personnes, qu'il aura désignées en donnant l'étendue de leur mandat, sont les mandataires de certification.

À défaut de désignation, le représentant légal est l'unique mandataire de certification.

Lors de l'enregistrement, l'organisation doit apporter la preuve de son existence, la preuve de l'identité de son représentant légal ainsi que la chaîne des mandats conférant leur pouvoir aux mandataires de certification.

L'AE doit archiver toutes les informations pertinentes relatives à cet enregistrement.

Général
La demande de certificat peut être adressée à l'AE au format papier signé manuscritement ou au format électronique, si possible signée à l'aide d'un procédé de signature électronique avancée.

3.2.1 Méthode pour prouver la possession de la clé privée

L'AC ne doit pas générer les clés des serveurs ; celle-ci doit vérifier que le demandeur est véritablement en possession de la clé privée associée à la clé publique qui sera inscrite dans son certificat. Cette vérification doit être réalisée à partir d'une demande de certificat au format PKCS#10 signée à l'aide de ladite clé privée.

Les demandes de certificat au format PKCS#10 doivent utiliser un algorithme de signature se basant sur un algorithme de hachage de la famille SHA2.

3.2.2 Validation de l'identité d'un organisme

Sauf pour les certificats DVCP, pour lesquels seules les informations relatives aux noms de domaines (FQDN) sont vérifiées, des vérifications relatives à l'identité de l'organisation sont effectuées par l'AE.

Le certificat doit toujours contenir le nom de l'entité identifiée (excepté pour les certificats DVCP) et, éventuellement, toutes les informations complémentaires permettant d'identifier son titulaire sans ambiguïté.

Général (sauf DVCP)
Vérification de l'identité d'un organisme

L'AE doit vérifier que la demande contient les pièces suivantes :

- Une autorisation d'émission signée, et datée de moins de 3 mois, par un représentant légal de l'entité ou par le mandataire de certification désignant le futur porteur bénéficiaire auquel le certificat doit être délivré,
- Une demande de certificat signée, et datée de moins de 3 mois, par le futur porteur bénéficiaire,
- Les conditions générales d'utilisation signées par le futur porteur bénéficiaire.
- SOIT pour une société enregistrée au registre du commerce français
  - un extrait K-Bis délivré par le greffe.
  - tout document attestant de la qualité du signataire de la demande de certificat
- SOIT pour un organisme français inscrit au répertoire SIRENE
  - un avis de situation au répertoire SIRENE justifiant du numéro d'enregistrement
  - un exemplaire des statuts / procès-verbal de l'assemblée générale, ou tout autre document en cours de validité portant signature des représentants de l'organisme
  - REPRESENTANTS ELUS : la copie des minutes / des délibérations nommant le Maire, Président etc. Cette copie devra comporter le cachet de votre organisme et la mention « certifiée conforme à l'original »
  - REPRESENTANTS NOMMES : copie du journal ou du bulletin officiel attestant cette nomination (merci de surligner la ligne en question, si la page contient beaucoup de texte).

Pour les sociétés enregistrées au registre du commerce français, l'AE peut le cas échéant se procurer par ses propres moyens un extrait K-Bis délivré par le greffe.

L'AE doit conserver les pièces reçues pour l'enregistrement du bénéficiaire, examine les pièces et documents remis avec un soin raisonnable et vérifie s'ils présentent ou non l'apparence de conformité et de validité.

Vérification du DBA et nom commercial

Si les informations sur l'identité du bénéficiaire doivent inclure un DBA ou un nom commercial, l'AE doit vérifier le droit du demandeur d'utiliser le DBA[2] / nom commercial à l'aide d'une des méthodes définies dans le référentiel [BRG] au chapitre 3.2.2.2.

Vérification du pays

Si le champ « subject :countryName » est présent dans le certificat, l'AE doit vérifier l'association du pays avec le bénéficiaire à l'aide d'une des méthodes définies dans le référentiel [BRG] au chapitre 3.2.2.3.

[2] Le nom commercial (en anglais DBA, "doing business as") est une "superposition" qui renvoie au nom officiel de votre entreprise

Uniquement pour les certificats QEVCP-w
Vérification de l'existence légale d'un organisme
L'AE doit vérifier que l'organisme existe et correspond à la demande à l'aide des bases de données officielles. Pour les organisations privées, l'AE vérifie l'exactitude et la cohérence des éléments suivants : - L'existence légale : l'entité est légalement reconnue, et son statut n'est pas « inactif », « invalide » ou « obsolète » - Le nom de l'organisation : le nom officiel enregistré est bien le même que dans la demande - Le numéro d'enregistrement : le numéro d'enregistrement, ou la date de constitution ou d'enregistrement de l'organisme le cas échéant - Le représentant légal : le nom et l'adresse du représentant légal Pour les entités publiques : - L'existence légale : l'entité est une entité gouvernementale légalement reconnue, existant dans la subdivision politique dans laquelle elle opère - Le nom de l'entité : le nom officiel enregistré est bien le même que dans la demande - Le numéro d'enregistrement : la date de constitution ou d'enregistrement de l'entité, ou l'identifiant de l'acte législatif qui a créé l'entité gouvernementale le cas échéant. Si ces éléments ne sont pas disponibles, le DN mentionnera de façon claire qu'il s'agit d'une entité publique Pour les entités commerciales : - L'existence légale : l'entité exerce une activité commerciale sous le nom soumis dans la demande - Le nom de l'entité : le nom officiel enregistré est bien le même que dans la demande - Le numéro d'enregistrement : le numéro d'enregistrement, ou la date d'enregistrement de l'entité le cas échéant - Le représentant légal : l'identité du représentant légal de l'entité Pour les entités non commerciales : - L'existence légale : l'entité est une entité légalement reconnue comme une organisation internationale - Le nom de l'entité : le nom officiel enregistré est bien le même que dans la demande - Le numéro d'enregistrement : la date de constitution de l'entité, ou l'identifiant de l'acte législatif qui a créé l'entité le cas échéant. Si ces éléments ne sont pas disponibles, le DN mentionnera de façon claire que l'entité est une organisation internationale
Vérification de l'existence physique de l'entité
L'AE doit vérifier que l'adresse physique fournie dans la demande est une adresse utilisée directement ou indirectement par l'organisation. L'AE utilise une des méthodes définies dans le référentiel [EVCG] au chapitre 3.2.2.4.1.
Vérification des moyens de communication de l'entité
L'AE doit vérifier un moyen de contact de communication de l'entité en utilisant une des méthodes définies dans le référentiel [EVCG] au chapitre 3.2.2.5.2.
Vérification de l'existence opérationnelle de l'entité
L'AE doit vérifier l'existence opérationnelle de l'entité en utilisant une des méthodes définies dans le référentiel [EVCG] au chapitre 3.2.2.6.2.
Vérification du nom de domaine de l'entité
Voir au chapitre 3.2.3.6 de la présente PC.

3.2.3 Validation de l'identité d'un individu

Pour toute demande de certificat faite au titre de l'appartenance à une organisation, il faut que ladite demande soit signée par le mandataire de certification et que les pièces justificatives soient envoyées à Certinomis.

Pour les certificats d'AC, toute demande de certificat doit être faite auprès de l'AE par le responsable de l'AC. Toute demande fait l'objet d'un script de cérémonie des clés, et d'un procès-verbal de cérémonie des clés, attestation de la génération des clés d'AC.

La validation de l'identité d'un individu concerne les personnes suivantes :

- Responsable de Certificat (RC)
- Mandataire de Certification (MC)
- Représentant légal

3.2.3.1 Enregistrement d'un RC sans MC pour un certificat de service applicatif à émettre

L'enregistrement du futur RC représentant une entité nécessite l'identification de cette entité, l'identification de la "personne physique" du futur RC, la vérification de son habilitation à être RC pour le service applicatif considéré et pour l'entité considérée, la justification de l'appartenance du nom de domaine du serveur (FQDN) à l'entité et la justification de l'existence d'une application au sein de l'entité.

L'identification de la personne physique responsable du dispositif (ou RC) est décrite ci-après.

Pour les certificats OVCP, QNCP-w et QEVCP-w
L'AE doit vérifier que la demande contient les pièces suivantes : • Un mandat signé, et daté de moins de 3 mois, par le responsable légal désignant le futur RC comme étant habilité à être responsable pour le service applicatif pour lequel le certificat doit être délivré. Ce mandat doit être signé par le représentant légal de l'entité et co-signé par le futur RC pour acceptation. • Un document officiel d'identité en cours de validité du futur RC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour). • L'adresse mail permettant à l'AC de contacter le RC. L'AE doit vérifier la photocopie d'au moins une pièce d'identité officielle du MC en cours de validité comportant sa photo et sa signature. Si la demande est transmise sous forme dématérialisée, l'AE doit vérifier que les documents sont signés à l'aide d'un procédé de signature électronique et que la signature soit valide au moment de l'enregistrement. L'AE doit conserver les pièces reçues pour l'enregistrement du bénéficiaire, examiner les pièces et documents remis avec un soin raisonnable et vérifier s'ils présentent ou non l'apparence de conformité et de validité. Si le dossier d'enregistrement est transmis au format papier, l'AE doit vérifier la photocopie d'au moins une pièce d'identité en cours de validité du futur bénéficiaire ou une carte professionnelle délivrée par une autorité administrative, comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour). Si le dossier d'enregistrement est dématérialisé, l'AE doit vérifier que le dossier est signé à l'aide d'un procédé de signature électronique conforme aux exigences du niveau RGS (*) et que la signature est valide au moment de l'enregistrement. L'AE doit conserver les pièces reçues pour l'enregistrement du bénéficiaire, examine les pièces et documents remis avec un soin raisonnable et vérifie s'ils présentent ou non l'apparence de conformité et de validité.

Uniquement pour les certificats QNCP-w et QEVCP-w
L'AE doit vérifier soit : • En face à face, c'est-à-dire en présence du RC, un original d'une pièce d'identité officielle du RC en cours de validité comportant sa photo et sa signature ; • Que le RC a communiqué dans son dossier de demande une attestation électronique de l'identité du futur bénéficiaire émise par une eID notifiée au minimum au niveau substantiel par un État membre de l'Union Européenne et délivrée en face à face ; • L'identité du MC à l'aide d'un Prestataire de Vérification d'Identité à Distance (PVID) certifié par l'ANSSI. Pour les certificats QEVCP-w, les éléments suivants doivent également être vérifiés lors du face-à-face : - Déclaration personnelle qui comprend les informations suivantes : o Nom complet o Adresse résidentielle à laquelle il/elle peut se trouver o Une affirmation que toutes les informations contenues dans la demande de certificat sont correctes - Au moins deux pièces justificatives secondaires dont l'une doit provenir d'une institution financière o Documents acceptables d'une institution financière ▪ Carte de crédit non expirée ▪ Carte de débit non expirée ▪ Relevé hypothécaire d'un prêteur reconnu datant de moins de six mois ▪ Relevé bancaire d'une institution financière réglementée datant de moins de six mois o Documents non financiers acceptables ▪ Factures de services publics originales récentes ou certificats d'une entreprise de services publics confirmant l'accord de paiement des services à une adresse fixe ▪ Copie d'une preuve de paiement d'un bail datant de moins de six mois ▪ Copie certifiée conforme d'une ordonnance du tribunal, telle qu'un certificat de divorce, des documents d'annulation ou des documents d'adoption
Uniquement pour les certificats DVCP
Seule la vérification de l'identité du dispositif décrite au chapitre 3.2.3.6 est nécessaire pour les certificats de niveau DVCP.

3.2.3.2 Enregistrement d'un nouveau RC sans MC pour un certificat déjà émis

L'enregistrement du nouveau RC (personne physique) représentant une entité nécessite l'identification de la personne physique et la vérification de son habilitation en tant que représentant de l'entité à laquelle le service applicatif est rattaché et en tant que RC pour le service applicatif considéré.

L'identification du nouveau RC est décrite au chapitre 3.2.3.1.

3.2.3.3 Enregistrement d'un Mandataire de Certification

Une AE est amenée à constituer un dossier d'enregistrement pour un Mandataire de Certification pour répondre aux besoins suivants :

- Utilisation du dossier du MC comme référence pour les données d'identification de l'entité de tous les bénéficiaires présentés par le MC ;
- Fourniture d'un certificat au MC pour qu'il puisse signer les dossiers d'enregistrement de certificats de services applicatifs de l'entité qu'il représente et les transmettre sous forme électronique.

L'identification du futur MC représentant une entité nécessite, d'une part, l'identification de cette entité et, d'autre part, l'identification de la personne physique.

L'identification de l'entité doit être réalisée suivant les modalités de l'article 3.2.2.

Général

L'AE doit vérifier que la demande contient les pièces suivantes :
• Un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le MC. Ce mandat doit être signé par le MC pour acceptation, contenant :
  • Un engagement du MC, auprès de l'AC, à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs,
  • Un engagement du MC à signaler à l'AE son départ de l'entité,
• Un document officiel d'identité en cours de validité du MC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie.
 	
L'AE doit vérifier la photocopie d'au moins une pièce d'identité officielle du MC en cours de validité comportant sa photo et sa signature.
 	
Si la demande est transmise sous forme dématérialisée, l'AE doit vérifier que les documents sont signés à l'aide d'un procédé de signature électronique conforme aux exigences du niveau RGS (*) et que la signature soit vérifiée et valide au moment de l'enregistrement.
 	
L'AE doit conserver les pièces reçues pour l'enregistrement du bénéficiaire, examine les pièces et documents remis avec un soin raisonnable et vérifie s'ils présentent ou non l'apparence de conformité et de validité.

Uniquement pour les certificats QNCP-w et QEVCP-w

L'AE doit vérifier soit :
• En face à face, c'est-à-dire en présence du MC, un original d'une pièce d'identité officielle du MC en cours de validité comportant sa photo et sa signature ;
• Que le MC a communiqué dans son dossier de demande une attestation électronique de l'identité du futur bénéficiaire émise par une eID notifiée au minimum au niveau substantiel par un État membre de l'Union Européenne et délivrée en face à face ;
• L'identité du MC à l'aide d'un Prestataire de Vérification d'Identité à Distance (PVID) certifié par l'ANSSI.
 	
Pour les certificats QEVCP-w, les éléments suivants doivent également être vérifiés lors du face-à-face :
- Déclaration personnelle qui comprend les informations suivantes :
  o Nom complet
  o Adresse résidentielle à laquelle il/elle peut se trouver
  o Une affirmation que toutes les informations contenues dans la demande de certificat sont correctes
- Au moins deux pièces justificatives secondaires dont l'une doit provenir d'une institution financière
  o Documents acceptables d'une institution financière
  ▪ Carte de crédit non expirée
  ▪ Carte de débit non expirée
  ▪ Relevé hypothécaire d'un prêteur reconnu datant de moins de six mois
  ▪ Relevé bancaire d'une institution financière réglementée datant de moins de six mois
  o Documents non financiers acceptables
  ▪ Factures de services publics originales récentes ou certificats d'une entreprise de services publics confirmant l'accord de paiement des services à une adresse fixe
  ▪ Copie d'une preuve de paiement d'un bail datant de moins de six mois
  ▪ Copie certifiée conforme d'une ordonnance du tribunal, telle qu'un certificat de divorce, des documents d'annulation ou des documents d'adoption

3.2.3.4 Enregistrement d'un RC via un MC pour un certificat à émettre

Le dossier d'enregistrement d'un RC doit être déposé au MC, qui le transmettra à l'AE. Lors de la transmission des dossiers de RC par le MC, celui-ci doit être authentifié auprès de l'AE :

- Soit à l'aide d'un certificat électronique remis par l'AC ;
- Soit au cours d'un face-à-face
- Soit par le paraphe du MC apposé sur les différentes pages du dossier de demande, complété par sa signature sur les principales pages

Général
L'AE doit vérifier que la demande contient les pièces suivantes : • Un mandat signé, et daté de moins de 3 mois, par le MC désignant le futur RC comme étant habilité à être responsable pour le service applicatif pour lequel le certificat doit être délivré. Ce mandat doit être signé par le MC et co-signé par le futur RC pour acceptation. • Un document officiel d'identité en cours de validité du futur RC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour). • L'adresse mail permettant à l'AC de contacter le RC. L'AE doit vérifier la photocopie d'au moins une pièce d'identité officielle du MC en cours de validité comportant sa photo et sa signature. Si la demande est transmise sous forme dématérialisée, l'AE doit vérifier que les documents sont signés à l'aide d'un procédé de signature électronique conforme aux exigences du niveau RGS (*) et que la signature soit vérifiée et valide au moment de l'enregistrement. L'AE doit conserver les pièces reçues pour l'enregistrement du bénéficiaire, examine les pièces et documents remis avec un soin raisonnable et vérifie s'ils présentent ou non l'apparence de conformité et de validité.
Uniquement pour les certificats QNCP-w et QEVCP-w
Le MC doit vérifier soit : • En face à face, c'est-à-dire en présence du RC, un original d'une pièce d'identité officielle du RC en cours de validité comportant sa photo et sa signature ; • Que le RC a communiqué dans son dossier de demande une attestation électronique de l'identité du futur bénéficiaire émise par une eID notifiée au minimum au niveau substantiel par un État membre de l'Union Européenne et délivrée en face à face ; • L'identité du RC à l'aide d'un Prestataire de Vérification d'Identité à Distance (PVID) certifié par l'ANSSI. Pour les certificats QEVCP-w, les éléments suivants doivent également être vérifiés lors du face-à-face : - Déclaration personnelle qui comprend les informations suivantes : o Nom complet o Adresse résidentielle à laquelle il/elle peut se trouver o Une affirmation que toutes les informations contenues dans la demande de certificat sont correctes - Au moins deux pièces justificatives secondaires dont l'une doit provenir d'une institution financière o Documents acceptables d'une institution financière ▪ Carte de crédit non expirée ▪ Carte de débit non expirée ▪ Relevé hypothécaire d'un prêteur reconnu datant de moins de six mois ▪ Relevé bancaire d'une institution financière réglementée datant de moins de six mois o Documents non financiers acceptables ▪ Factures de services publics originales récentes ou certificats d'une entreprise de services publics confirmant l'accord de paiement des services à une adresse fixe ▪ Copie d'une preuve de paiement d'un bail datant de moins de six mois ▪ Copie certifiée conforme d'une ordonnance du tribunal, telle qu'un certificat de divorce, des documents d'annulation ou des documents d'adoption

3.2.3.5 Enregistrement d'un nouveau RC pour un certificat déjà émis

Dans le cas de changement d'un RC en cours de validité d'un certificat serveur, le nouveau RC doit être enregistré en tant que tel par l'AC en remplacement de l'ancien RC.

L'identification du nouveau RC (personne physique) représentant une entité nécessite l'identification de la personne physique et la vérification de son habilitation en tant que représentant de l'entité à laquelle le serveur est rattaché et en tant que RC pour le serveur considéré. (cf. chapitre 3.2.3.1).

3.2.3.6 Enregistrement d'un dispositif ou d'une application

L'identification du futur dispositif (ou application) représentant une entité nécessite, d'une part, l'identification de cette entité et, d'autre part, l'identification de la personne physique responsable du dispositif et enfin l'identité du dispositif.

L'identification de l'entité et du responsable du dispositif doit être réalisée suivant les dispositions de l'article 3.2.3.1 et si l'entité désigne un MC suivant l'article 3.2.3.2.

L'AE doit vérifier que le demandeur est autorisé à recevoir des certificats pour le dispositif ou l'application. La personne ou l'organisation qui présente une demande doit établir la preuve de son droit d'usage sur le dispositif ou l'application dont mention sera faite dans le certificat. En particulier dans le cas d'un serveur web, elle devra établir la preuve que le nom de domaine lui appartient bien.

Vérification de l'identité du dispositif
L'AE doit vérifier que la demande contient les pièces suivantes : • Une autorisation d'émission signée, et datée de moins de 3 mois, par un représentant légal de l'entité ou par le mandataire de certification désignant le futur RC comme étant habilité à être RC pour le serveur informatique auquel le certificat serveur doit être délivré. • Une demande de certificat signée, et datée de moins de 3 mois, par le futur RC bénéficiaire comportant l'identité du serveur concerné par cette demande pour acceptation. • Les conditions générales d'utilisation signées par le futur RC. L'AE doit vérifier la possession par l'entité du nom de domaine correspondant au(x) FQDN pour les demandes de certificats d'authentification serveur. L'AE doit utiliser l'une des méthodes de validation définies dans le [BRG] suivantes : o 3.2.2.4.7 : changement DNS L'AE doit effectuer une vérification des enregistrements CAA telle que définie dans la RFC 8659 pour chaque nom de domaine présent dans l'extension « subjectAltName » du certificat à émettre. L'AE doit documenter les rejets de demande dus à la vérification CAA. L'utilisation d'adresse IP dans l'extension champ subjectAltName est interdit. L'utilisation d'un nom de domaine ".onion est interdit. L'AE doit conserver les pièces reçues pour l'enregistrement du dispositif, examine les pièces et documents remis avec un soin raisonnable et vérifie s'ils présentent ou non l'apparence de conformité et de validité.

3.2.4 Informations non vérifiées

Docaposte Certinomis SAS au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Sans objet.

3.2.5 Validation de l'autorité du demandeur

Cette étape doit être effectuée en même temps que la validation de l'identité de la personne physique (directement par l'AE ou par le MC).

3.2.6 Critères d'interopérabilité

Aucune certification croisée n'est établie avec d'autres ACs.

3.3 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES

Le renouvellement de la bi-clé d'un certificat entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni au bénéficiaire sans renouvellement de la bi-clé correspondante (cf. chapitre 5.6).

3.3.1 Identification et validation pour un renouvellement courant

Pour toute demande de renouvellement, la procédure de demande initiale s'applique.

3.3.2 Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial.

3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

La demande de révocation d'un certificat de bénéficiaire peut être effectuée sur le site web de Certinomis par le bénéficiaire ou par le mandataire du certificat. L'AE doit authentifier la demande avant traitement : vérification d'une ou deux informations de base du demandeur (adresse, n° de téléphone, etc.) et de son autorité par rapport au certificat à révoquer.

La demande peut également être adressée par courrier. Elle doit alors être signée par le demandeur et le service de gestion des révocations doit s'assurer de l'identité du demandeur (vérification de la signature manuscrite par rapport à une signature préalablement enregistrée) et de son autorité par rapport au certificat à révoquer.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

Le présent chapitre définit les pratiques opérationnelles relatives à la gestion des clés et des certificats.

4.1 DEMANDE DE CERTIFICAT

4.1.1 Origine d'une demande de certificat

L'AC publie sur son site web toutes les procédures et les exigences concernant une demande de certificat. Les demandeurs de certificat doivent suivre et respecter les procédures publiées.

Pour les bénéficiaires (RC), un certificat peut être demandé par un représentant légal de l'entité ou un MC dûment mandaté pour cette entité, avec dans tous les cas consentement préalable du futur bénéficiaire.

4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

4.1.2.1 Certificats d'AC

Les demandes sont effectuées par le responsable de l'AC, dans le cadre de la Cérémonie des clés.

4.1.2.2 Certificats de bénéficiaire

La demande d'identification électronique envoyée à l'AE doit au moins contenir l'adresse de courrier électronique du demandeur.

Chaque demande doit être associée à des pièces, elles aussi transmises à l'AE, qui permettent de prouver l'identité et les pouvoirs des futurs bénéficiaires conformément aux procédures applicables en fonction du type de certificat demandé (articles 3.2.2, 3.2.3 et 3.3), notamment :

- la preuve de l'identité du demandeur ;
- la preuve des pouvoirs pour les attributs demandés, par exemple d'appartenance à un organisme ou une société, de possession d'un nom de domaine ;
- le contrat client ou la référence à un contrat client préexistant

Dans le cas d'une organisation, pour chaque demande, il faut qu'il existe une autorisation d'émission signée d'un mandataire de certification identifié et un contrat client signé par un représentant habilité qui peut ne pas être mandataire de certification. Ce contrat doit faire mention des obligations d'information du bénéficiaire sur ses obligations.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

4.2.1 Exécution des processus d'identification et de validation de la demande

Une demande de certificat n'oblige en aucune façon l'AC à émettre un certificat.

L'émission d'un certificat par une AC indique que celle-ci a définitivement et complètement approuvé la demande de certificat.

Si la demande de certificat n'a pas pu être validée après 3 mois, celle-ci sera annulée par Certinomis (les documents justificatifs auront dépassé leur durée de validité de 3 mois).

Dans le cadre de la mise en œuvre du contrôle des enregistrements DNS de type CAA, la présente politique reconnaît uniquement les émetteurs (CAA issue / issuewild) ayant pour valeur « www.certinomis.com » (https://ccadb-public.secure.force.com/mozilla/CAAIdentifiersReport).

L'AE conserve ensuite une trace des justificatifs d'identité présentés.

4.2.2 Acceptation ou rejet de la demande

À la réception d'une demande de certificat, l'AC doit :

- s'assurer que la demande a bien été prise en compte par une AE qu'elle a reconnue et que ladite AE a traité la demande et fourni une trace imputable de son avis ;
- vérifier que les noms de domaines contenus dans la demande ne soient pas des noms internes (seuls les FQDN publics sont autorisés pour les certificats TLS/SSL).
- générer et signe le certificat.

En cas de rejet de la demande, l'AE en informe le bénéficiaire, et/ou le MC le cas échéant, en justifiant le rejet.

4.2.3 Durée d'établissement du certificat

Une fois la demande de certificat validée, le certificat doit être émis dans les meilleurs délais.

4.3 DELIVRANCE DU CERTIFICAT

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments destinés au bénéficiaire :

- Le bénéficiaire génère les clés et transmet la CSR à l'AC.
- L'AC génère le certificat.
- Le certificat est créé dans le système d'AC, un numéro unique lui est attribué.
- Un email est envoyé au bénéficiaire contenant son code d'autorévocation.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 5 et 6 ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre 5.2).

4.3.2 Notification par l'AC de la délivrance du certificat au RC

Le certificat peut être transmis par message électronique à une adresse fournie par le porteur, ou bien l'URL permettant de télécharger le certificat peut être envoyée à une telle adresse.

4.4 ACCEPTATION DU CERTIFICAT

4.4.1 Démarche d'acceptation du certificat

Une fois le certificat transmis, le bénéficiaire doit vérifier le contenu du certificat. La première utilisation du certificat vaut acceptation tacite dudit certificat. À défaut, le certificat est accepté tacitement 15 jours après l'émission du certificat.

En acceptant un certificat, le bénéficiaire reconnaît expressément consentir aux termes et aux conditions d'utilisation contractuelles et, plus généralement, à tous les éléments publiés dans la présente Politique de certification.

4.4.2 Publication du certificat

En dehors des pré-certificats inscrits dans les logs « Certificate Transparency », les certificats émis ne font pas l'objet d'une publication par l'AC.

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

L'AC informe l'AE de la délivrance du certificat, qui se charge d'en informer le MC le cas échéant.

4.5 USAGES DE LA BI-CLE ET DU CERTIFICAT

4.5.1 Utilisation de la clé privée et du certificat par le RC

Les bénéficiaires doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service défini par l'OID de sa politique (cf. chapitre 1.4.1.1).

4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Cf. paragraphe ci-dessus et chapitre 1.4.

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6 RENOUVELLEMENT D'UN CERTIFICAT

Nota -Conformément au [RFC3647], la notion de "renouvellement de certificat" correspond à la délivrance d'un nouveau certificat pour lequel seul les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique).

La présente PC impose que les certificats et les bi-clés correspondantes aient la même durée de vie, il ne peut donc pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé.

4.6.1 Circonstance pour le renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification de la délivrance d'un nouveau certificat

Sans objet.

4.6.5 Modalité d'acceptation d'un nouveau certificat

Sans objet.

4.6.6 Publication du renouvellement du certificat par l'AC

Sans objet.

4.6.7 Notification de la délivrance par l'AC aux autres entités

Sans objet.

4.7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE

Nota -Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat au bénéficiaire lié à la génération d'une nouvelle bi-clé.

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des serveurs, et les certificats correspondants, doivent être renouvelés au minimum tous les 397 jours.

Les bi-clés des AC devront être renouvelées au minimum tous les 6 ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat (cf. chapitre 4.9, notamment le chapitre 4.9.1.1 pour les différentes causes possibles de révocation).

4.7.2 Origine d'une demande d'un nouveau certificat

Toute demande de certificat est considérée et traitée comme une demande initiale.

Cf. chapitre 4.1.1.

4.7.3 Procédure de traitement d'une demande d'un nouveau certificat

Cf. chapitre 4.2.

4.7.4 Notification au bénéficiaire de l'établissement du nouveau certificat

Cf. chapitre 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1.

4.7.6 Publication du nouveau certificat

Cf. chapitre 4.4.2.

4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Cf. chapitre 4.4.3.

4.8 MODIFICATION DU CERTIFICAT

Nota -Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre 4.7) et autre qu'uniquement la modification des dates de validité (cf. chapitre 4.6).

La modification de certificat n'est pas autorisée dans la présente PC.

4.8.1 Circonstance pour la modification d'un certificat

Sans objet.

4.8.2 Origine d'une demande de modification de certificat

Sans objet.

4.8.3 Traitement d'une demande de modification de certificat

Sans objet.

4.8.4 Notification de la délivrance d'un nouveau certificat

Sans objet.

4.8.5 Modalité d'acceptation d'un certificat modifié

Sans objet.

4.8.6 Publication du certificat modifié par l'AC

Sans objet.

4.8.7 Notification par l'AC aux autres entités de la délivrance du certificat

Sans objet.

4.9 REVOCATION ET SUSPENSION DES CERTIFICATS

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats de bénéficiaires

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat électronique :

- les informations du service figurant dans le certificat ne sont plus en conformité avec l'identité du service ou l'utilisation prévue dans le certificat (par exemple, modification du FQDN), ceci avant l'expiration normale du certificat ;
- l'AC obtient la preuve qu'il ne faut pas se fier à la validation de l'autorisation ou du contrôle du domaine pour tout FQDN présent dans le certificat ;
- le RC n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le RC et/ou, le cas échéant, le MC / l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- la clé privée du service applicatif est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- l'AC est informée d'une méthode démontrée ou éprouvée qui peut facilement calculer la clé privée du service applicatif sur la base de la clé publique du certificat ;
- le RC ou une entité autorisée (représentant légal de l'entité ou MC par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du service applicatif et/ou de son support) ;
- le RC informe l'AC que la demande de certificat n'a pas été autorisée et n'accorde pas d'autorisation rétroactive ;
- l'arrêt définitif du service applicatif ou la cessation d'activité de l'entité du RC de rattachement du service applicatif ;
- il n'y a plus de RC identifié pour le certificat électronique.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

4.9.1.2 Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats, de LCR) :

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la PC ou la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant la composante.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats de bénéficiaires

Seuls peuvent demander la révocation d'un certificat :

- le bénéficiaire, responsable du certificat ;
- le mandataire de certification ou le représentant légal de l'entité ;
- le personnel de l'AC émettrice ;
- le personnel de l'AE qui a enregistré la demande du bénéficiaire.

Le bénéficiaire est informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat dans les conditions générales d'utilisation et sur le site web de Certinomis.

4.9.2.2 Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité responsable de l'AC.

4.9.3 Procédure de traitement d'une demande de révocation

Les motifs de la révocation d'un certificat donné ne sont jamais divulgués à des tiers sauf en cas d'accord écrit du bénéficiaire ou du client.

Dans le cadre des audits et contrôles auxquels l'AC est soumise en vertu de la présente politique de certification, des éléments sur les motifs de révocation, non nominatifs et non liés à un certificat, pourront être fournis. D'une manière plus générale, ces éléments pourront être utilisés à des fins statistiques.

4.9.3.1 Révocation d'un certificat de bénéficiaire

L'AC offre un moyen d'accès rapide, électronique ou téléphonique, au service de révocation qui authentifiera la demande dans des conditions fixées au chapitre 3. Ce service de révocation pourra être assuré directement par l'AC ou par une AE reconnue par l'AC.

La demande de révocation doit contenir les informations d'identification du certificat à révoquer. La demande peut également contenir la description détaillée des causes de la révocation, et, éventuellement, les justificatifs de cette cause. La procédure de révocation est détaillée sur ce site : https://www.certinomis.fr/revoquer-votre-certificat.

Si la procédure de demande de révocation d'un certificat est justifiée et se déroule correctement, la révocation est déclenchée. L'ensemble des opérations et des mesures prises par l'AC doit être consigné et sauvegardé.

Quelle que soit la cause ayant entraîné la révocation d'un certificat, le bénéficiaire doit toujours être informé par une notification de la révocation de son certificat. Dans le cas d'une organisation, le mandataire de certification peut également être notifié. Cette notification doit indiquer la date à laquelle la révocation du certificat a pris effet. Elle peut prendre la forme d'un courrier électronique.

4.9.3.2 Révocation d'un certificat d'une composante de l'IGC

En cas de révocation d'un des certificats de la chaîne de certification, l'AC doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des bénéficiaires concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE et aux MC. Ces derniers devront informer les bénéficiaires de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides, car un des certificats de la chaîne de certification n'est plus valide.

La révocation du certificat de l'AC est facilitée par la signature d'une LAR par l'autorité de certificat racine.

Le point de contact identifié sur le site et le CCADB doivent immédiatement être informés en cas de révocation d'un des certificats de la chaîne de certification.

4.9.4 Délai accordé au RC pour formuler la demande de révocation

Dès que le bénéficiaire (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

4.9.5 Délai de traitement par l'AC d'une demande de révocation

4.9.5.1 Révocation d'un certificat de bénéficiaire

Par nature une demande de révocation doit être traitée en urgence.

La fonction de gestion des révocations doit être disponible 24h/24 7j/7.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 1h et une durée maximale totale d'indisponibilité par mois de 4h.

Toute demande de révocation d'un certificat doit être traitée dans un délai inférieur à 24h, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

Si toutefois, la demande de révocation ne pouvait pas être traitée dans le délai des 24h stipulé précédemment, un nouveau délai de révocation sera calculé en fonction de la situation rencontrée et le demandeur sera contacté avant l'expiration du délai stipulé, afin de lui indiquer le nouveau délai exceptionnel de révocation.

4.9.5.2 Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC doit être effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats

Avant toute utilisation de certificats, notamment lorsque lesdits certificats créent des effets juridiques, le tiers utilisateur doit impérativement vérifier la validité des certificats auxquels elle entend se fier auprès de Certinomis, en consultant les Listes des Certificats Révoqués valides les plus récentes ainsi qu'en contrôlant la validité intrinsèque du certificat, en particulier sa signature, et la validité du certificat de l'émetteur.

La validité d'une LCR est contrôlée par vérification de sa signature et vérification de la validité du certificat de l'émetteur.

4.9.7 Fréquence d'établissement et durée de validité des LAR/LCR

Une nouvelle LAR doit être émise à minima une fois par an. Une nouvelle LAR doit être émise suivant la révocation d'un certificat d'AC.

Une nouvelle LCR doit être émise à minima toutes les 24 heures. Une nouvelle LCR peut être émise suivant la révocation d'un certificat de bénéficiaire.

4.9.8 Délai maximum de publication d'une LAR/LCR

Une LCR ou une LAR doit être publiée dans un délai maximum de 30 minutes suivant sa génération.

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Une publication complémentaire suivant le protocole OCSP doit être disponible pour les certificats de bénéficiaire.

4.9.10 Exigences de vérification en ligne de la révocation des certificats

Cf. chapitre 4.9.6 et 4.9.9 ci-dessus.

4.9.11 Autres moyens disponibles d'information sur les révocations

Aucun autre moyen n'est disponible.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

En cas de compromission avérée ou soupçonnée de la clé privée de signature d'une AC, l'AC doit aviser sans tarder toutes les autorités qui l'accréditent.
La connaissance de la compromission avérée ou soupçonnée de la clé privée, par le client ou le bénéficiaire emporte obligation de procéder sans délai à la vérification de la révocation du certificat associé et de la demander dans les plus brefs délais si celle-ci n'a pas été faite.

La procédure de révocation d'une AC doit être réalisée par une opération de cérémonie de clé.

4.9.13 Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

4.10.1 Caractéristiques opérationnelles

L'AC doit fournir aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR et l'état du certificat de l'AC Racine.

Lorsqu'un service de LCR/LAR est proposé, alors celles-ci doivent être au format V2.

4.10.2 Disponibilité de la fonction d'information sur l'état des certificats

La fonction d'information sur l'état des certificats doit être disponible 24h/24 7j/7.
Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h et une durée maximale totale d'indisponibilité par mois de 8h.

4.10.3 Dispositifs optionnels

Aucun dispositif optionnel n'est disponible.

4.11 FIN DE LA RELATION ENTRE LE RC ET L'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et le l'entité de rattachement du service applicatif, avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.
De plus, l'AC doit révoquer un certificat pour lequel il n'y a plus de RC explicitement identifié.

4.12 SEQUESTRE DE CLE ET RECOUVREMENT

Les clés privées des bénéficiaires ne doivent pas être séquestrées.
Les clés privées d'AC ne doivent pas être séquestrées.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

5 MESURES DE SECURITE NON TECHNIQUES

5.1 MESURES DE SECURITE PHYSIQUE

Les locaux techniques, qui accueillent les moyens de certification et notamment sa clé privée de signature, doivent être fortement protégés contre les intrusions.

Le niveau de protection des locaux techniques est essentiel dans la garantie de la sécurité des moyens de certification et de leur exploitation.

5.1.1 Situation géographique et construction des sites

La présente PC ne formule pas d'exigence spécifique concernant la localisation géographique.

La construction des sites doit respecter les règlements et normes en vigueur et le cas échéant, des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques...).

5.1.2 Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès aux locaux des différentes composantes de l'IGC doivent être contrôlés.

L'accès doit être strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines doit être limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

Nota -On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisé pour la mise en œuvre de ces fonctions.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation doivent permettre de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

Elles doivent également permettre de respecter les exigences de la présente PC, ainsi que les engagements pris par l'AC dans sa DPC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux doivent permettre de respecter les exigences de la présente PC, ainsi que les engagements pris par l'AC dans sa DPC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies doivent permettre de respecter les exigences de la présente PC, ainsi que les engagements pris par l'AC dans sa DPC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.6 Conservation des supports

Dans le cadre de l'analyse de risque, les différentes informations intervenant dans les activités de l'IGC doivent être identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

L'AC doit maintenir un inventaire de ces informations. L'AC doit mettre en place des mesures pour éviter la compromission et le vol de ces informations.

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations doivent être gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils doivent être manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion doivent protéger ces supports contre l'obsolescence et la détérioration pendant la période durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

5.1.7 Mise hors service des supports

En fin de vie, les supports devront être, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

Les procédures et moyens de destruction et de réinitialisation doivent être conformes à ce niveau de confidentialité.

5.1.8 Sauvegardes

Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, doivent mettre en œuvre des sauvegardes déportées permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.).

Les informations sauvegardées doivent respecter les mêmes exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.

5.2 MESURES DE SECURITE PROCEDURALES

5.2.1 Rôles de confiance

Chaque composante de l'IGC distingue au moins les sept rôles fonctionnels de confiance suivants :

Responsable de sécurité - Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

Responsable d'application - Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

Ingénieur système - Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.

Opérateur - Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.

Contrôleur - Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

Opérateur d'enregistrement - L'opérateur d'enregistrement cumule les fonctions d'officier d'enregistrement et officier de révocation. Il est chargé de valider les demandes de certificat, et de traiter les demandes de révocation des certificats de bénéficiaire.

Spécialiste validation – Le spécialiste validation est chargé de réaliser les vérifications requises par les [BRG] et [EVCG].

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, l'AC distingue également en tant que rôle de confiance, les rôles de porteur de parts de secrets d'IGC : cf. chapitres 6.1 et 6.2.

Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiées.

5.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, les fonctions sensibles sont réparties sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC (cf. chapitre 6)

La DPC précise les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter.

5.2.3 Identification et authentification pour chaque rôle

Tous les membres du personnel de l'AC doivent faire vérifier leur identité et leurs autorisations avant :

•que leur nom soit ajouté à la liste d'accès aux locaux de l'AC ; ou

•que leur nom soit ajouté à la liste des personnes autorisées à accéder physiquement au système de l'AC.

Tous les intervenants sur le système de l'AC, ou d'une autre composante de l'IGC, doivent faire vérifier leur identité et leur autorisation avant :

- qu'un certificat leur soit délivré pour accomplir le rôle qui leur est dévolu ; ou
- qu'un compte soit ouvert en leur nom dans le système.

Chacun de ces certificats et comptes (à l'exception des certificats de signatures de l'AC) :

- est attribué directement à une personne ;
- ne dois pas être partagé ;
- dois être utilisé seulement pour les tâches **autorisées** pour le rôle assigné ; un mécanisme de contrôle est mis en place.

Les opérateurs distants intervenant sur le système de l'AC doivent être identifiés au moyen de mécanismes cryptographiques forts.

L'AC et les composantes de l'IGC s'assurent que tout processus de vérification qu'elles utilisent permet de superviser toutes les activités des personnes qui en leur sein détiennent des rôles privilégiés.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur
- contrôleur et tout autre rôle
- ingénieur système et opérateur

5.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

5.3.1 Qualifications, compétences et habilitations requises

Le responsable de l'AC doit s'assurer que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation d'une AC, qu'ils dépendent de l'AC directement, de l'AE :

- sont nommés à un poste faisant l'objet d'une description détaillée par écrit ;
- sont liés par contrat ou par la loi aux postes qu'ils occupent ;
- ont reçu toute la formation nécessaire pour accomplir leurs tâches ;
- sont tenus par contrat ou par la loi de ne pas divulguer de renseignements ayant trait à la sécurité de l'AC, aux clients ou aux bénéficiaires ; une clause de confidentialité est expressément inscrite dans les contrats de travail des membres du personnel de l'AC ;

Des obligations identiques sont portées à la charge du responsable de l'AE et d'en communiquer le résultat à l'AC.

5.3.2 Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC doit mettre en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.

A ce titre, l'employeur peut demander à ces personnels la communication d'une copie du bulletin n°3 de leur casier judiciaire.

L'employeur peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions du personnel, de lui retirer ces attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications doivent être menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

5.3.3 Exigences en matière de formation initiale

Le personnel doit être préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné doit recevoir une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Les sanctions doivent être précisées dans la DPC.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC doit également respecter les exigences du présent chapitre 5.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8 Documentation fournie au personnel

Chaque personnel doit disposer au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, il doit lui être remis la ou les politique(s) de sécurité l'impactant

5.4 PROCEDURES DE CONSTITUTION DES DONNÉES D'AUDIT

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier ou électronique, rendent possibles la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'évènements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre de l'IGC, chaque entité opérant une composante de l'IGC doit au minimum journaliser les évènements tels que décrits ci- dessous, sous forme électronique. La journalisation doit être automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements doivent aussi être recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration des systèmes ;
- les changements apportés au personnel ;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les RC,...).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment :

- réception d'une demande de certificat (initiale et renouvellement) ;
- validation / rejet d'une demande de certificat ;
- évènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,…) ;
- le cas échéant, génération des éléments secrets du service applicatif (bi-clé, codes d'activation,…) ;
- génération des certificats de services applicatifs;transmission des certificats aux RC et, selon les cas, acceptations / rejets explicites par les RC ;
- le cas échéant, remise du dispositif de protection du service applicatif au RC ;
- publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- réception d'une demande de révocation ;
- validation / rejet d'une demande de révocation ;
- génération puis publication des LCR (et éventuellement des deltaLCR) ou des, requêtes / réponses OCSP ;

Chaque enregistrement d'un évènement dans un journal doit contenir au minimum les champs suivants :

- type de l'évènement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) ;
- résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'évènement ;
- toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation doivent être effectuées au cours du processus.
En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

Les évènements et données spécifiques à journaliser doivent être documentés par l'AC.

5.4.2 Fréquence de traitement des journaux d'évènements

Cf. chapitre 5.4.8.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements doivent être conservés sur site pendant au moins un (1) mois. Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard sous un (1) mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

5.4.4 Protection des journaux d'évènements

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système de datation des évènements doit respecter les exigences du chapitre VI.8.

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.5 Procédure de sauvegarde des journaux d'évènements

Chaque entité opérant une composante de l'IGC doit mettre en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC.

5.4.6 Système de collecte des journaux d'évènements

Sans objet.

5.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

5.4.8 Évaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC doit être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements doivent être contrôlés une (1) fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux doivent être analysés dans leur totalité au minimum une fois toutes les deux semaines et dès la détection d'une anomalie.

Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) doit être effectué au moins une fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

5.5 ARCHIVAGE DES DONNEES

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage doivent également être prises par l'AC. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les conditions générales d'utilisation ;
- les accords contractuels avec d'autres AC ;
- les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les engagements signés des MC ;
- les justificatifs d'identité des bénéficiaires et, le cas échéant, de leur entité de rattachement ;
- les justificatifs d'identité des services applicatifs ;
- les journaux d'évènements des différentes entités de l'IGC (notamment le cycle de vie des certificats et des clés d'AC).

5.5.2 Période de conservation des archives

5.5.2.1 Dossiers de demande de certificat

Tout dossier de demande de certificat accepté doit être archivé aussi longtemps que nécessaire, et pendant au moins sept (7) ans, pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi française.

Lorsque les RC sont enregistrés par une autorité d'enregistrement dans un autre pays que celui ou l'AC est établie, alors il convient que cette AE applique également la réglementation de son propre pays.

Lorsque des MC sont également dans un autre pays, alors il convient de prendre également en compte les exigences contractuelles et légales applicables à ces MC.

La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du RC ou du MC.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.

Ce dossier, complété par les mentions consignées par l'AE ou le MC, doit permettre de retrouver l'identité réelle du RC responsable, à un instant "t" du service applicatif désigné dans le certificat émis par l'AC.

5.5.2.2 Certificats, LCR et réponses OCSP émis par l'AC

Les certificats de services applicatifs et d'AC, ainsi que les LCR / LAR, doivent être archivés pendant au moins cinq (5) années après leur expiration.

Les réponses OCSP produites doivent être archivées pendant au moins trois mois après leur expiration.

5.5.2.3 Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 doivent être archivés pendant dix (10) années après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage doivent offrir le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements doit être assurée tout au long de leur cycle de vie.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :

- être protégées en intégrité ;
- être accessibles aux personnes autorisées ;
- pouvoir être relues et exploitées.

L'AC précisera dans sa DPC internes les moyens mis en œuvre pour archiver les pièces en toute sécurité.
Une copie de tout le matériel informatique archivé ou sauvegardé est protégée soit par des mesures de sécurité physique seulement, soit par une combinaison de mesures physiques et cryptographiques. Le site d'archivage protège adéquatement le matériel contre les dangers naturels, par exemple les excès de température, d'humidité et de magnétisme.

L'AC vérifiera l'intégrité de ses archives au moins tous les six (6) mois.

De plus, les informations conservées ou sauvegardées par l'AC peuvent être assujetties aux lois et règlements en vigueur et applicables à l'archivage et la conservation.

5.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

5.5.5 Exigences d'horodatage des données

Cf. chapitre 5.4.4 pour la datation des journaux d'évènements.
Le chapitre 6.8 précise les exigences en matière de datation / horodatage.

5.5.6 Système de collecte des archives

Le système de collecte des archives, qu'il soit interne ou externe, doit respecter les exigences de protection des archives concernées.

5.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à deux (2) jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

5.6 CHANGEMENT DE CLE D'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.

Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée doit être utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé, et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

Le certificat ne peut être prorogé au-delà de sa date de validité. Donc, l'émission d'un nouveau certificat nécessitera un renouvellement des clés.

5.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

Chaque entité opérant une composante de l'IGC doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …). L'AC doit également prévenir directement et sans délai, le point de contact identifié sur le site https://cyber.gouv.fr.

Toute pratique non-conforme avec la PC ou la DPC internes en vigueur doit être considérée comme un incident. Une non-conformité majeure dans le cadre d'un audit de certification doit également être considérée comme un incident.

Tout incident doit faire l'objet d'un rapport d'incident et doit être communiqué à qui de droit.

La procédure de traitement des incidents doit être précisée dans la DPC internes.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses serveurs devient insuffisant pour son utilisation prévue restante, alors l'AC doit :

- informer tous les RC et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou à d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- révoquer tout certificat concerné.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)

Chaque composante de l'IGC doit disposer d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la PC Type RGS, des engagements de l'AC dans sa propre PC notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan doit être testé au minimum une fois tous les deux ans.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante doit être traité dans le plan de continuité de la composante (cf. chapitre 5.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué : cf. chapitre IV.9.

En outre, l'AC doit au minimum respecter les engagements suivants :

- informer les entités suivantes de la compromission : tous les RC, MC et les autres entités avec lesquelles l'AC a passé des accords ou a d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information doit être mise à disposition des autres tiers utilisateurs ;
- indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC.

5.8 FIN DE VIE DE L'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC doit prendre les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

5.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC doit entre autres obligations :

- Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des bénéficiaires et des informations relatives aux certificats) ;
- Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la PC.
- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire sous un délai d'un mois;
- L'AC doit communiquer au point de contact identifié sur le site https://cyber.gouv.fr/, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC devra communiquer à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats ;
- L'AC doit tenir informée l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

5.8.2 Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité est progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprennent les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans la présente PC.

L'AC doit stipuler dans ses pratiques les dispositions prises en cas de cessation de service. Elles doivent inclure :

- La notification des entités affectées ;
- Le transfert de ses obligations à d'autres parties ;
- La gestion du statut de révocation pour les certificats non expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC doit :

- S'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- Prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- Révoquer son certificat ;
- Révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- Informer (par exemple par récépissé) tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

6 MESURES DE SECURITE TECHNIQUES

Le présent chapitre a pour objet de définir les dispositions de gestion des bi-clés de l'AC, du personnel de l'AC, des AE déléguées, et des bénéficiaires.

6.1 GENERATION ET INSTALLATION DE BI-CLES

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

La génération des clés de signature d'AC doit être effectuée dans un environnement sécurisé (cf. chapitre 5).

Les clés de signature d'AC doivent être générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature d'AC doit être effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. Chapitre 5.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies doivent se dérouler suivant des scripts préalablement définis.

L'initialisation de l'IGC et/ou la génération des clés de signature d'AC peut s'accompagner de la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.

Ces parts de secrets doivent être générées suivant un schéma à seuil de Shamir (n parties parmi m sont nécessaires et suffisantes pour reconstituer le secret), ce secret permet de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la (ou des) clé(s) privée(s) d'AC sauvegardée(s) lors de la cérémonie de clés.

Suite à leur génération, les parts de secrets doivent être remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur.

Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est un auditeur qualifié au sens du [BRG].

Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

6.1.1.2 Clés du service applicatif générées par l'AC

Sans objet.

6.1.1.3 Clés du service applicatif générées au niveau du service applicatif

Lorsque la bi-clé est générée au niveau du serveur, cette génération doit être effectuée dans un dispositif répondant aux exigences du chapitre 12 ci-dessous. L'AC doit s'en assurer auprès du RC, au travers d'un engagement contractuel du responsable du serveur vis-à-vis de l'AC.

Les demandes pour lesquelles les bi-clés ne correspondant pas aux types et tailles de clés autorisés dans la présente PC au chapitre 7 doivent être rejetées.

6.1.2 Transmission de la clé privée au RC

Sans objet.

6.1.3 Transmission de la clé publique à l'AC

En cas de transmission de la requête de demande de certificat de service applicatif au format PKCS10, ou tout autre conteneur offrant les mêmes garanties de sécurité, vers une composante de l'AC (cas où la bi- clé est générée au niveau du service applicatif), la clé devra être protégée en intégrité et son origine devra en être authentifiée.

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les clés publiques de vérification de signature de l'AC doivent être diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

Une clé publique d'AC peut être diffusée dans un certificat qui est soit un certificat racine autosigné, soit un certificat rattaché à une hiérarchie d'AC jusqu'à une AC racine (cf. chapitre I.4.1.2 ci-dessus).

Un certificat racine autosigné ne permet pas de garantir par lui-même que la clé publique correspondante appartient bien à l'AC considérée. Sa diffusion doit s'accompagner de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat, et éventuellement de la clé publique, ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC.

La clé publique de l'AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) doivent pouvoir être récupérées aisément par les utilisateurs de certificats.

6.1.5 Tailles des clés

Les clés d'AC et de services applicatifs doivent respecter les exigences de caractéristiques précisées ci-dessous :

Clés d'AC Racine
Type de clé : RSA Taille de la clé : 4096 bits
Clés d'AC intermédiaire
Type de clé : RSA Taille de la clé : 4096 bits
Clés de certificat de bénéficiaire
Type de clé : NIST P-256 Taille de la clé : 256 bits ou Type de clé : RSA Taille de la clé : minimum 3072 bits

6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité

Le moyen de génération de la bi-clé doit utiliser des paramètres respectant les normes internationales de sécurité propres à l'algorithme considéré. En particulier, les paramètres des bi-clés doivent être conformes aux spécifications du document [SOGIS-CRYPTO].

Pour les clés de type RSA, l'exposant public doit être un nombre impair supérieur à 2^{16}. La taille du module doit être supérieure ou égal à 3072 bits pour un certificat émis à partir du 1er janvier 2026.

Pour les clés de type courbe elliptique, les courbes suivantes sont autorisées : NIST P-256, NIST P-384, NIST P-512.

6.1.7 Objectifs d'usage de la clé

Les différents usages possibles des clés publiques sont définis et ainsi contraints par l'utilisation d'une extension de certificat X.509 v.3 (champ KeyUsage).

La clé publique de vérification de l'AC est la seule clé utilisable pour vérifier la signature des certificats.

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR et/ou de réponses OCSP (cf. chapitre 1.4.1.2 et 7.1.2).

L'utilisation de la clé privée et du certificat émis associé est strictement limitée au service défini dans les chapitres 1.4.1.1, 4.5 et 7.1.2.

6.2 MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

Le bénéficiaire doit protéger ses clés privées afin qu'elles ne soient pas divulguées. Il lui appartiendra de s'assurer qu'une maintenance particulière est réalisée sur le serveur utilisé ; en particulier de la stabilité du système, de l'absence de virus, vers et chevaux de Troie. Il lui appartient également de choisir le matériel et les logiciels offrant une sécurité suffisante pour la protection et l'utilisation de ses clés privées conformément aux dispositions du présent chapitre 6.

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature, ainsi que le cas échéant pour la génération des clés des futurs certificats, doivent être des modules cryptographiques répondant au minimum aux exigences du chapitre 11 ci-dessous.

6.2.1.2 Dispositifs cryptographiques du service applicatif

Les dispositifs d'utilisation et de protection de clés privées des serveurs, pour la mise en œuvre de leurs clés privées, doivent respecter les exigences du chapitre 12 ci-dessous.

Lorsque le dispositif cryptographique est fourni par le client, l'AC doit s'assurer auprès du responsable du serveur de la conformité du dispositif mis en œuvre par le serveur, au travers d'un engagement contractuel clair et explicite du RC vis-à-vis de l'AC.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la bi-clé est traitée au chapitre 6.1.1.1, l'activation de la clé privée au chapitre 6.2.8 et sa destruction au chapitre 6.2.10.

Le contrôle des clés privées de signature de l'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 3).

6.2.3 Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des services applicatifs ne doivent en aucun cas être séquestrées.

6.2.4 Copie de secours de la clé privée

Les clés privées des services applicatifs ou d'AC peuvent faire l'objet de copie de secours.

Ces copies peuvent être effectuées soit dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée.

Les opérations de chiffrement et de déchiffrement doivent être effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.

Le contrôle des opérations de chiffrement / déchiffrement doit être conforme aux exigences du chapitre 6.2.2.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC ne doivent en aucun cas être archivée.

Les clés privées des services applicatifs ne doivent en aucun cas être archivées ni par l'AC ni par aucune des composantes de l'IGC.

6.2.6 Transfert de la clé privée vers / depuis le module cryptographique

6.2.6.1 Clés privées des Autorités

Pour les clés privées d'AC, tout transfert doit se faire sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.6.2 Clés privées des serveurs

Sans objet.

6.2.7 Stockage de la clé privée dans un module cryptographique

Il est recommandé de stocker les clés privées d'AC dans un module cryptographique répondant au minimum aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

Cependant, dans le cas des copies de secours, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences du chapitre 6.2.4.

Quel que soit le moyen utilisé, l'AC doit garantir que les clés privées d'AC ne sont pas compromises pendant leur stockage ou leur transport.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'AC

La méthode d'activation des clés privées d'AC dans un module cryptographique doit permettre de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

L'activation des clés privées d'AC dans le module cryptographique doit être contrôlée via des données d'activation (cf. chapitre 6.4) et doit faire intervenir au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).

6.2.8.2 Clés privées des services applicatifs

Sans objet.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

La désactivation des clés privées d'AC dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc. Une clé privée d'AC peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

6.2.9.2 Clés privées des services applicatifs

Sans objet.

6.2.10 Méthode de destruction des clés privées

6.2.10.1Clés privées d'AC

La méthode de destruction des clés privées d'AC doit permettre de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.
En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé doit être systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.10.2Clés privées des services applicatifs

La destruction des clés privées des bénéficiaires est sous la responsabilité du bénéficiaire.

6.2.11 Niveau d'évaluation sécurité du module cryptographique

Pour les clés d'AC, le niveau d'évaluation du module cryptographique est précisé au chapitre 11.

Le niveau d'évaluation des modules cryptographiques des services applicatifs est précisé au chapitre 12 ci-dessous.

6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1 Archivage des clés publiques

L'AC émettrice archive ou fait archiver toutes les clés publiques de vérification conformément à l'article 5.5.

6.3.2 Durées de vie des bi-clés et des certificats

L'utilisation d'une longueur particulière de clé est déterminée conformément à l'évaluation de la menace et des risques prenant en compte l'évolution des technologies d'attaque.

6.3.2.1 Bi-clés et certificats d'AC

La bi-clé et le certificat de l'AC Racine doivent avoir une durée de vie maximale de 25 ans.
Les bi-clés et les certificats des AC intermédiaires doivent avoir une durée de vie maximale de 6 ans.

6.3.2.2 Bi-clés et certificats de bénéficiaire

Les bi-clés et les certificats des services applicatifs doivent avoir une durée de vie maximale de 397 jours.

6.4 DONNEES D'ACTIVATION

6.4.1 Génération et installation des données d'activation

6.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC doivent se faire lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles doivent leur être transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne doivent être connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre 5.2.1).

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du service applicatif

Sans objet.

6.4.2 Protection des données d'activation

6.4.2.1 Protection des données d'activation correspondant à la clé privée de l'AC

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'IGC doivent être protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.2.2 Protection des données d'activation correspondant aux clés privées des services applicatifs

Sans objet.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC doit être défini dans la DPC internes de l'AC. Il doit au moins répondre aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique),
- gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels,
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- protection du réseau contre toute intrusion d'une personne non autorisée,
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- fonctions d'audits (non-répudiation et nature des actions effectuées),
- éventuellement, gestion des reprises sur erreur.

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle (cf. chapitre 1.4.1.2) doit faire l'objet de mesures particulières, qui peuvent découler de l'analyse de risque.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) doivent être mis en place.

L'AC doit mettre en conformité ses pratiques avec les documents de l'ANSSI relatifs à la protection du poste de l'application de l'AE et du poste de l'AC.

En particulier, l'AC doit appliquer l'ensemble des règles définies dans le guide d'hygiène informatique publié par l'ANSSI pour le niveau « standard ».

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Sans objet.

6.6 MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

6.6.1 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC doit être documentée et doit respecter dans la mesure du possible des normes de modélisation et d'implémentation. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau doivent être documentées et contrôlées.

L'AC doit :

- garantir que les objectifs de sécurité sont définis lors des phases de spécification et de conception,
- utiliser des systèmes et des produits fiables qui sont protégés contre toute modification.

6.6.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC doit être signalée à l'AC pour validation. Elle doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

6.7 MESURES DE SECURITE RESEAU

L'interconnexion vers des réseaux publics doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

L'AC doit garantir que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC.

De plus, les échanges entre composantes au sein de l'IGC peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

6.8 HORODATAGE / SYSTEME DE DATATION

Plusieurs exigences de la présente PC nécessitent la datation par les différentes composantes de l'IGC d'évènements liés aux activités de l'IGC (cf. chapitre 5.4).

Pour dater ces évènements, les différentes composantes de l'IGC peuvent recourir :

- soit à une autorité d'horodatage, interne ou externe à l'IGC, conforme aux exigences du référentiel ETSI EN 319 421 ;
- soit en utilisant l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près. Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les évènements avec une précision suffisante. Pour la synchronisation par rapport au temps UTC, il est recommandé de se référer à un système comprenant au moins deux sources indépendantes de temps.

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

Le contenu des certificats et des LCR est conforme aux exigences de la RFC 5280 : « Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile ».

7.1 PROFIL DES CERTIFICATS

7.1.1 Certificats d'AC

7.1.1.1 AC Racine

Champ	C	Contenu/Présent/Absent
Version	N	3 (0x2)
Serial Number	N	*Valeur aléatoire générée par l'AC*
Signature Algorithm	N	Sha256WithRSAEncryption
Issuer DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
Subject DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
Validity	N	25 ans
Subject Public Key Info	N	RSA 4096 bits
Key Usage	O	keyCertSign, cRLSign
Basic Constraints	O	cA=True
Authority Key Identifier	N	*Identifiant de la clé publique de l'AC Racine*
Subject Key Identifier	N	*Identifiant de la clé publique de l'AC Racine*

7.1.1.2 AC Intermédiaires

7.1.1.2.1 AC Web G2

Champ	C	Contenu/Présent/Absent
Version	N	3 (0x2)
Serial Number	N	*Valeur aléatoire générée par l'AC*
Signature Algorithm	N	Sha256WithRSAEncryption
Issuer DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
Subject DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web CA G2
Validity	N	6 ans maximum
Subject Public Key Info	N	RSA 4096 bits
Key Usage	O	keyCertSign, cRLSign
Basic Constraints	O	cA=True pathLen = 0
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ac-racine-web-root-ca.cer

Authority Key Identifier	N	*Identifiant de la clé publique de l'AC Racine*
Subject Key Identifier	N	*Identifiant de la clé publique de l'AC*
Certificate Policies	N	Policy = X509v3 AnyPolicy
CRL Distribution Points	N	URI=http://www.certinomis.com/publi/crl/ac-racine-web-root-ca.crl
Extended Key Usage	N	id-kp-serverAuth, id-kp-clientAuth

7.1.1.2.2 AC Safe G2

Champ	C	Contenu/Présent/Absent
Version	N	3 (0x2)
Serial Number	N	*Valeur aléatoire générée par l'AC*
Signature Algorithm	N	Sha256WithRSAEncryption
Issuer DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
Subject DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Safe CA G2
Validity	N	6 ans maximum
Subject Public Key Info	N	RSA 4096 bits
Key Usage	O	keyCertSign, cRLSign
Basic Constraints	O	cA=True pathLen = 0
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ac-racine-web-root-ca.cer
Authority Key Identifier	N	*Identifiant de la clé publique de l'AC Racine*
Subject Key Identifier	N	*Identifiant de la clé publique de l'AC*
Certificate Policies	N	Policy = X509v3 AnyPolicy
CRL Distribution Points	N	URI=http://www.certinomis.com/publi/crl/ac-racine-web-root-ca.crl
Extended Key Usage	N	id-kp-serverAuth, id-kp-clientAuth

7.1.2 Certificats de bénéficiaire

7.1.2.1 Champs de base

Les champs x509 suivants sont communs à l'ensemble des certificats de bénéficiaire :

Champ	C	Contenu/Présent/Absent
Version	N	3 (0x2)
Serial Number	N	*Valeur aléatoire générée par l'AC*
Signature Algorithm	N	Sha256WithRSAEncryption
Validity	N	*397 jours maximum*
Subject	N	*Cf. 7.1.2.2*
Issuer	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = *Nom commun de l'AC émettrice (Certinomis – Safe CA G2 ou Certinomis Web CA G2)*

Subject Public Key Info	N	*Elliptic Curve P-256, RSA 3072 bits, ou RSA 4096 bits*
Key Usage	O	digitalSignature
Authority Key Identifier	N	*Identifiant de la clé publique de l'AC émettrice*
Subject Key Identifier	N	*Identifiant de la clé publique du porteur*
Basic Constraints	O	False
Subject Alternative Name (Adresse RFC822 : DNS)	N	*Ensemble FQDN des domaines demandés et validés*
CT Precertificate SCTs	N	*Liste d'entrées SCTs.*

7.1.2.2 Noms uniques des porteurs

Les noms uniques des porteurs (Subject DN) sont définis selon le tableau suivant :

	QNCP-w	QEVCP-w	OVCP RGS *	OVCP	DVCP
countryName	Pays dans lequel l'entité du porteur est enregistrée				
stateOrProvince	Département de domiciliation de l'entité du porteur				
localityName	Commune de domiciliation de l'entité du porteur				
organizationName	Nom ou raison sociale de l'entité du porteur				
commonName	Un des FQDN présent dans l'extension SAN				
organizationIdentifier	Identifiant de l'entité du porteur telle que définie à la section 5.1.4 du standard ETSI EN 319 412-1.				
serialNumber	Numéro unique généré par l'AC				

En plus de ces éléments, le DN des certificats QEVCP-w comporte les champs suivants :

businessCategory	"Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" selon le type d'entité légale du porteur
jurisdictionLocalityName	Commune de juridiction de l'entité du porteur (si pertinent)
jurisdictionStateOrProvinceName	Département de juridiction de l'entité du porteur (si pertinent)
jurisdictionCountryName	Pays de juridiction de l'entité du porteur

Note : ces informations sont renseignées par l'opérateur d'enregistrement en fonction de

7.1.2.3 Pré-certificats

L'AC Certinomis émet des pré-certificats préalablement à l'émission de tout certificat porteur. Ces pré-certificats contiennent l'ensemble des champs et extensions qui seront présents dans le certificat final, à l'exception de l'extension « CT Precertificate SCTs ». Le SCT obtenu par la publication du pré-certificat est inclus dans le certificat final dans cette extension.

7.1.2.4 OID 1.2.250.1.86.2.6.8.62.1 – QNCP-w

Champ	C	Contenu/Présent/Absent
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.86.2.6.8.62.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques

CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-safe-g2.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-safe-g2.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth, id-kp-clientAuth
Qc Compliance	N	id-etsi-qcs-QcCompliance id-etsi-qcs-QcPDS = https://www.certinomis.fr/documents-et-liens/nos-conditions-generales-dutilisation id-etsi-qcs-QcType = id-etsi-qct-web

7.1.2.5 OID 1.2.250.1.86.2.6.8.63.1 – QEVCP-W

Champ	C	Contenu/Présent/Absent
Certificate Policies	N	2.23.140.1.1 1.2.250.1.86.2.6.8.63.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-safe-g2.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-safe-g2.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth, id-kp-clientAuth
Qc Compliance	N	id-etsi-qcs-QcCompliance id-etsi-qcs-QcPDS = https://www.certinomis.fr/documents-et-liens/nos-conditions-generales-dutilisation id-etsi-qcs-QcType = id-etsi-qct-web

7.1.2.6 OID 1.2.250.1.86.2.6.7.20.1 – OVCP RGS *

Champ	C	Contenu/Présent/Absent
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.86.2.6.7.20.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-web-g2.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-web-g2.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth

7.1.2.7 OID 1.2.250.1.86.2.6.7.61.1 – OVCP

Champ	C	Contenu/Présent/Absent
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.86.2.6.7.61.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-web-g2.crl

Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-web-g2.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth, id-kp-clientAuth

7.1.2.8 OID 1.2.250.1.86.2.6.7.60.1 – DVCP

Champ	C	Contenu/Présent/Absent
Certificate Policies	N	2.23.140.1.2.1 1.2.250.1.86.2.6.7.60.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-web-g2.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-web-g2.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth, id-kp-clientAuth

7.1.2.9 Certificats OCSP

Champ	C	Contenu/Présent/Absent
Version	N	3 (0x2)
Serial Number	N	*Numéro unique généré par l'AC*
Signature Algorithm	N	Sha256WithRSAEncryption
Validity	N	*3 ans maximum*
Subject	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = CERTINOMIS - WEB G2 OCSP (ou CERTINOMIS – SAFE G2 OCSP)
Issuer	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = *Nom commun de l'AC émettrice (Certinomis – Safe CA G2 ou Certinomis Web CA G2)*
Subject Public Key Info	N	*Elliptic Curve P-256, RSA 3072 bits, ou RSA 4096 bits*
Key Usage	O	digitalSignature
Authority Key Identifier	N	*Identifiant de la clé publique de l'AC émettrice*
Subject Key Identifier	N	*Identifiant de la clé publique du certificat*
Basic Constraints	N	False
Subject Alternative Name (Adresse RFC822 : DNS)	N	
Authority Information Access	N	
Extended Key Usage	N	id-kp-OCSPSigning

7.2 PROFIL DES LCR/LAR

7.2.1 Profil des LAR

7.2.1.1 Champs de base

Champ	Contenu
Version	2 (0x1)
Signature	Sha256WithRSAEncryption

Issuer	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
This Update	*Date d'émission de la LAR*
Next Update	*Date d'émission de la prochaine LAR (1 an maximum après la date d'émission)*
Revoked Certificates	- userCertificate : *numéro de série unique du certificat révoqué* - revocationDate : *date de la révocation* - revocationCause : *cause de la révocation*

7.2.1.2 Extensions

Champ	C	Contenu
Authority Key Identifier	N	*Identifiant de la clé publique de l'AC émettrice de la LCR*
CRL Number	N	*Numéro de série de la LCR*

7.2.2 Profil des LCR

7.2.2.1 AC SAFE G2

7.2.2.1.1 Champs de base

Champ	Contenu
Version	2 (0x1)
Signature	Sha256WithRSAEncryption
Issuer	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Safe CA G2
This Update	*Date d'émission de la LCR*
Next Update	*Date d'émission de la prochaine LCR (7 jours maximum après la date d'émission)*
Revoked Certificates	- userCertificate : *numéro de série unique du certificat révoqué* - revocationDate : *date de la révocation* - revocationCause : *cause de la révocation (champ présent uniquement si la cause de la révocation est l'une des suivantes : keyCompromise, privilegeWithdrawn, cessationOfOperation, affiliationChanged, superseded)*

7.2.2.1.2 Extensions

Champ	C	Contenu
Authority Key Identifier	N	*Identifiant de la clé publique de l'AC émettrice de la LCR*
CRL Number	N	*Numéro de série de la LCR*
ExpiredCertsOnCRL	N	*Date à partir de laquelle les certificats révoqués et expirés sont conservés dans la LCR*

7.2.2.2 AC WEB G2

7.2.2.2.1 Champs de base

Champ	Contenu
Version	2 (0x1)
Signature	Sha256WithRSAEncryption

Issuer	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web CA G2
This Update	*Date d'émission de la LCR*
Next Update	*Date d'émission de la prochaine LCR*
Revoked Certificates	- userCertificate : *numéro de série unique du certificat révoqué* - revocationDate : *date de la révocation*

7.2.2.2.2 Extensions

Champ	C	Contenu
Authority Key Identifier	N	*Identifiant de la clé publique de l'AC émettrice de la LCR*
CRL Number	N	*Numéro de série de la LCR*

7.3 PROFIL DES REPONSES OCSP

7.3.1.1 Champs de base

Champ	Contenu
OCSP Response Status	*Code de réponse tel que défini dans la RFC 6960*
Version	1 (0x0)
Responder Id	*Identifiant de la clé publique du répondeur OCSP*
Produced At	*Date à laquelle le répondeur OCSP a signé la réponse*
Certificate ID	- Hash Algorithm: sha1 - Issuer Name Hash : *Hash du DN de l'AC émettrice* - Issuer Key Hash : *Identifiant de la clé publique de l'AC émettrice* - Serial Number : *Numéro de série du certificat*
Cert Status	*Good, revoked ou unknown tel que défini dans la RFC 6960*
This Update	*Date la plus récente à laquelle la réponse indiquée est connue par le répondeur comme étant correcte*
Next Update	*Date avant laquelle de nouvelles informations sur l'état du certificat seront disponibles (entre 24h et 7 jours après la date contenue dans le champ « This Update »)*
Signature Algorithm	sha256WithRSAEncryption ou ecdsaWithSHA256

7.3.1.2 Extensions

Champ	C	Contenu
OCSP Archive Cutoff	N	*Date à partir de laquelle le statut des certificats expirés et révoqués est conservé par le répondeur*
OCSP Nonce	N	*Contient la valeur du champ « Nonce » si présent dans la requête OCSP*

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Le présent chapitre ne concerne que les audits et évaluations de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

8.1 FREQUENCES ET/OU CIRCONSTANCES DES EVALUATIONS

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC doit procéder à un contrôle de conformité de cette composante.

L'AC doit également procéder annuellement à un contrôle de conformité de l'ensemble de son IGC.

8.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

Le contrôle d'une composante doit être assigné par l'AC à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

8.3 RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

L'équipe d'audit ne peut pas appartenir à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

8.4 SUJETS COUVERTS PAR LES EVALUATIONS

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définis dans la présente PC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants :

- "réussite",
- "échec",
- "à confirmer".

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.
- En cas de résultat "À confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la présente PC et la DPC associée.

8.6 COMMUNICATION DES RESULTATS

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

Si le rapport d'audit contient des informations touchant la sécurité de l'AC ou des informations qu'elles considèrent confidentielles, la publication n'est pas effectuée. Il est possible d'obtenir, sur demande expresse, un résumé ou des extraits du rapport sous forme électronique.

Les attestations d'audits de conformité sont tenues à la disposition du public. Il est possible d'obtenir, sur demande expresse, une copie sous forme électronique.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 TARIFS

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Des frais d'émission de certificat seront facturés selon une échelle de tarifs diffusés par l'AC sur son site WEB, ou négociés dans le cadre d'un contrat commercial.

9.1.2 Tarifs pour accéder aux certificats

Des frais d'accès au certificat peuvent être facturés par l'AC selon une échelle de tarifs diffusés ou négociés avec l'AC.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

Des frais de vérification de validité des certificats peuvent être facturés par l'AC selon une échelle des tarifs diffusés ou négociés avec l'AC.

Un moyen gratuit de contrôle du statut du certificat est toujours laissé à la disposition du tiers utilisateur (LCR en téléchargement sur le site web de Certinomis).

9.1.4 Tarifs pour d'autres services

Aucuns frais ne seront facturés pour l'accès en direct à cette Politique de Certification ou à la DPC. Cependant, des frais peuvent être facturés pour des copies sur support papier ou par voie électronique.

9.1.5 Politique de remboursement

Aucune exigence particulière.

9.2 RESPONSABILITE FINANCIERE

9.2.1 Couverture par les assurances

La garantie associée au certificat est limitée au montant prévu au contrat. Pour toute transaction commerciale, ou échange électronique, dont les conséquences financières directes ou indirectes sont d'un montant supérieur au montant prévu, la responsabilité des acteurs de l'IGC ne peut être engagée vis-à-vis des clients, bénéficiaires et tiers utilisateurs.

9.2.2 Autres ressources

Aucune exigence particulière.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Les certificats garantis par la présente PC comportent un niveau d'assurance garanti, précisé par contrat et accessible à la partie utilisatrice.

9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- les clés privées de l'AC, des composantes et des certificats émis,
- les données d'activation associées aux clés privées de l'AC et des certificats émis[3],
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- le dossier d'enregistrement du client,
- les causes de révocation, sauf accord explicite de publication ;
- les procédures et politiques internes de Certinomis.

9.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre IX.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'AC doit en garantir l'intégrité.

L'AC est tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des certificats de services applicatifs à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au RC et au MC.

9.4 PROTECTION DES DONNEES PERSONNELLES

9.4.1 Politique de protection des données personnelles

Le Règlement Européen UE 2016/679 du 27 avril 2016 relatif à la protection des données personnelles ainsi que la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifié par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel s'applique à tous les documents détenus ou transmis par l'AC ou par une des composantes de l'IGC (site de la CNIL http://www.cnil.fr).

En vertu des textes, les clients et les bénéficiaires disposent d'un droit d'accès, de rectification et d'opposition à la cession de toute information qui les concerne. Ce droit peut s'exercer par l'intermédiaire du service agent, en particulier l'AE, ayant recueilli ces informations, à l'adresse figurant sur le site WEB de l'AC.

L'AC respecte rigoureusement toutes les prescriptions légales applicables et explique sur son site WEB, les modalités concrètes d'application de la loi, notamment dans les rubriques « mentions légales & gestion des données personnelles ».

[3] La confidentialité des données d'activation des clés privées des certificats émis est garantie par l'AC tant qu'elle les détient.

La Politique de Certification respecte les principes fondamentaux en matière de protection des données à caractère personnel consacrés dans la loi, le RGPD et toute autre convention internationale entrée en vigueur.

9.4.2 Données à caractère personnel

Toutes les données collectées et détenues par l'AC ou une AE sur une personne physique ou morale (par exemple : procédure d'enregistrement, révocation, autres évènements consignés, correspondances échangées entre le bénéficiaire et l'AC ou l'AE, etc.) sont considérées comme confidentielles et ne peuvent pas être divulguées sans avoir obtenu le consentement préalable du bénéficiaire.

Les renseignements concernant l'identification ou d'autres données à caractère personnel, du bénéficiaire, apparaissant sur les certificats sont considérés comme étant confidentiels, sauf si le bénéficiaire a donné son consentement exprès et préalable à toute diffusion.

Les Listes des Certificats Révoqués ne contiennent que les numéros d'enregistrement des certificats, et leur date de révocation. Les causes de révocation des certificats sont réputées demeurer strictement confidentielles.

9.4.3 Données à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données à caractère personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous)

9.4.5 Notification et consentement d'utilisation des données à caractère personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous)

9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous)

9.4.7 Autres circonstances de divulgation de données personnelles

Le secret des correspondances émises par voie des télécommunications est garanti par la loi française. En cas d'atteinte, toute violation est punie par l'article 226-15 du code pénal pour celles commises par un particulier et par les articles 432-9 et 432-17 du code pénal pour celles commises par une personne dépositaire de l'autorité publique.

D'une façon générale, aucun salarié de l'AC et aucun collaborateur ou sous-traitant, dans le cadre de leur participation aux services de certification, n'a le droit d'intercepter, d'ouvrir, de détourner, de divulguer, de rechercher ou d'utiliser les documents soumis à l'AC, sauf dans les cas prévus dans la présente politique, ou dans le cadre du régime des interceptions ordonnées par l'autorité judiciaire ou des interceptions de sécurité en vertu de la loi n°91-646 du 10 juillet 1991.

9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE

9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Ce chapitre contient des dispositions relatives aux obligations respectives de l'AC, du personnel de l'AC, des diverses entités composant l'IGC, des clients, des bénéficiaires et des tiers utilisateurs. Elle contient aussi des dispositions juridiques, relatives notamment à la loi applicable et à la résolution des litiges.

Les obligations communes aux composantes de l'IGC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre VIII) et l'organisme de qualification,
- respecter les accords ou contrats qui les lient entre elles ou aux RC,
- documenter leurs procédures internes de fonctionnement,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1 Autorités de Certification

L'AC a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un service applicatif donné et que le RC correspondant a accepté le certificat, conformément aux exigences du chapitre IV.4 ci-dessus.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses RC sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un RC et l'AC est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC est responsable de la conformité de sa Politique de Certification, avec les exigences émises dans les référentiels applicables pour le niveau de sécurité considéré. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, par elle-même ou l'une de ses composantes. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des RC à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AC.

9.6.2 Service d'enregistrement

Cf. les obligations pertinentes du chapitre 9.1.

9.6.2.1 Obligations du mandataire de certification

Le mandataire de certification doit se conformer à toutes les exigences de la présente Politique de Certification.

Il s'engage à respecter le contrat qui le lie à l'AC.

Il garantit que les informations qu'il fournit à l'AC ou à une AE, pour l'identification de l'entité identifiée ou du bénéficiaire, sont exactes, complètes et que les documents transmis ou présentés sont valides.

Le mandataire de certification doit établir et faire respecter une politique de sécurité sur les postes informatiques utilisés pour mettre en œuvre les certificats.

S'il soupçonne la compromission d'une clé privée, il est tenu d'en aviser l'AC dans les plus brefs délais et selon les instructions données par celle-ci.

Il doit protéger en confidentialité et en intégrité ses clés privées, ses codes d'activation ou d'accès. Il doit prendre toutes les mesures raisonnables pour en éviter la perte, la divulgation, la compromission, la modification ou l'utilisation non autorisée.

9.6.3 Bénéficiaire de certificats

Le bénéficiaire doit se conformer à toutes les exigences de la présente Politique de Certification.

Il s'engage à respecter le contrat qui le lie à l'AC.

Il garantit que les informations qu'il fournit à l'AC ou à une AE, pour son identification, celle du bénéficiaire ou de l'entité identifiée, sont exactes, complètes et que les documents transmis ou présentés sont valides.

Si le bénéficiaire est une organisation, il doit établir et faire respecter une politique de sécurité sur les postes informatiques utilisés pour mettre en œuvre les certificats.
S'il soupçonne la compromission d'une clé privée, il est tenu d'en aviser l'AC dans les plus brefs délais et selon les instructions données par celle-ci.

En aucun cas le bénéficiaire n'acquiert la propriété du certificat émis par l'AC. Il n'en acquiert que le droit d'usage. Par conséquent, tous les certificats demeurent la propriété de l'AC qui les a émis.

9.6.4 Utilisateurs de certificats

L'utilisateur doit se conformer à toutes les exigences de la présente Politique de Certification. Le bénéficiaire doit exclusivement utiliser ses clés privées et certificats à des fins autorisées par la présente Politique de Certification, ainsi que dans le respect des lois et règlements en vigueur.

Il garantit que les informations qu'il fournit à l'AC ou à une AE, pour son identification ou celle de l'entité identifiée, sont exactes, complètes et que les documents transmis ou présentés sont valides.

Il doit protéger en confidentialité et en intégrité ses clés privées, ses codes d'activation ou d'accès conformément à l'article 6.2. Il doit prendre toutes les mesures raisonnables pour en éviter la perte, la divulgation, la

compromission, la modification ou l'utilisation non autorisée. Il s'engage à suivre toute prescription du client en matière de politique de sécurité dans le cadre de l'usage du certificat.

S'il soupçonne la compromission d'une clé privée, il est tenu d'en aviser l'AC dans les plus brefs délais et selon les instructions données par celle-ci.

9.6.5 Autres participants

9.6.5.1 Obligation du tiers utilisateur

Avant toute utilisation de certificats, notamment lorsque lesdits certificats créent des effets juridiques, le tiers utilisateur doit impérativement avoir un comportement raisonnable : vérifier la validité des certificats auxquels il entend se fier auprès de Certinomis, en consultant les Listes des Certificats Révoqués appropriées les plus récentes, ainsi qu'en vérifiant leur date d'expiration et leur validité intrinsèque, en particulier sa signature, et la validité de tout certificat sur l'itinéraire de confiance. À défaut de remplir cette obligation, le tiers utilisateur assume seul tous les risques de ses actions non conformes aux exigences de la présente politique, Certinomis ne garantissant aucune valeur juridique aux certificats qu'elle a émis et qui pourraient avoir été révoqués ou qui ne seraient pas valides.

En outre, lors de la vérification d'une signature électronique, le tiers utilisateur doit aussi vérifier que la clé publique du certificat correspond à la clé privée de signature utilisée.

Le tiers utilisateur doit toujours vérifier que le certificat est utilisé à des fins pertinentes et conformément aux applications autorisées.

Un tiers utilisateur ne doit utiliser les certificats que conformément à la procédure de validation de l'itinéraire de confiance, procédure qui est spécifiée dans les normes X. 509 et PKIX et déterminée par la recommandation ISO/IEC 9594-8.

9.7 LIMITE DE GARANTIE

L'émission de certificats, conformément à la présente Politique de Certification, ne fait pas de l'AC, de l'une des composantes de l'IGC, du responsable de l'AC et du personnel de l'AC et des composantes de l'IGC un fiduciaire, un mandataire, un garant ou un autre représentant de quelque façon que ce soit du bénéficiaire, du client ou de toutes autres parties concernées. Chaque partie s'interdit de prendre un engagement au nom et pour le compte de l'autre partie à laquelle elle ne saurait en aucun cas se substituer.

En conséquence de quoi, les bénéficiaires, les mandataires de certification, les clients et les tiers utilisateurs de certificat sont des personnes juridiquement et financièrement indépendantes et, à ce titre, ne disposent d'aucun pouvoir ni de représentation, ni d'engager l'AC ou l'une des composantes de l'IGC, susceptible de créer des obligations juridiques, tant de façon expresse que tacite au nom de l'AC ou de l'une des composantes de l'IGC. Les services de certification ne constituent pas un partenariat ni ne créent une quelconque forme juridique d'association juridique qui imposerait une responsabilité basée sur les actions ou les carences de l'autre. Le contrat ne constitue ni une association, ni une société ou autre groupement, ni un mandat donné par l'une des parties à l'autre.

Le fait que le nom d'une organisation soit dans un certificat de signature électronique ne constitue pas en soi un mandat spécial ou général de cette organisation en faveur du bénéficiaire.

La garantie associée au certificat est limitée au montant prévu au contrat. Pour toute transaction commerciale, ou échange électronique, dont les conséquences financières directes ou indirectes sont d'un montant supérieur au montant prévu, la responsabilité des acteurs de l'IGC ne peut être engagée vis-à-vis des clients, bénéficiaires et tiers utilisateurs.

Docaposte Certinomis SAS au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

9.8 LIMITE DE RESPONSABILITE

L'AC, le personnel de l'AC, les composantes de l'IGC, les clients, les bénéficiaires, les tiers utilisateurs sont responsables pour tous dommages et intérêts découlant du non-respect de leurs obligations respectives telles que définies aux termes de la présente Politique de Certification et de la DPC associée.

L'AC détaille le périmètre des limites de responsabilité dans sa DPC.

9.9 INDEMNITES

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de l'une des parties envers l'autre, les dommages et intérêts et indemnités à sa charge, toutes causes confondues, ne sauraient en aucun cas dépasser les limites de responsabilité mentionnées dans le cadre du contrat conclu entre l'AC et son client.

9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1 Durée de validité

La présente PC reste en application jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

La publication d'une nouvelle version de la présente PC peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa DPC correspondante.

En fonction de la nature et de l'importance des évolutions apportées à la PC, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

9.10.3 Effets de la fin de validité et clauses restant applicables

Sans objet.

9.11 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes ;
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

9.12 AMENDEMENTS A LA PC

Le présent chapitre définit les exigences en matière d'administration et de gestion de la présente politique de certification.

9.12.1 Procédures d'amendements

L'AC devra contrôler que tout projet de modification de sa PC reste conforme aux exigences de la PC type RGS, aux exigences des référentiels ETSI applicables, aux exigences du [BRG], et des éventuels documents complémentaires. En cas de changement important, l'AC fera appel à une expertise technique pour en contrôler l'impact.

9.12.2 Mécanisme et période d'information sur les amendements

Pas d'exigence particulière.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des RC, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

En particulier, l'OID de la PC de l'AC doit évoluer dès lors qu'un changement majeur intervient dans les exigences applicable à la famille de certificats considérée.

9.13 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

L'AC doit mettre en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles elle fournit des services électroniques de confiance ou d'autres points qui y sont liés.

9.14 JURIDICTIONS COMPETENTES

La présente politique de certification est expressément élaborée, régie, appliquée et interprétée selon les lois et règlements français, bien que les activités qui découlent de la présente Politique de Certification puissent avoir des effets juridiques en dehors du territoire de la République française.

9.15 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 10 ci-dessous.

9.16 DISPOSITIONS DIVERSES

9.16.1 Accord global

Sans objet.

9.16.2 Transfert d'activités

Cf. chapitre 5.8.

9.16.3 Conséquences d'une clause non valide

Le caractère inapplicable dans un contexte donné d'une disposition de la Politique de Certification n'affecte en rien la validité des autres dispositions, ni de cette disposition hors du dit contexte. La Politique de Certification continue à s'appliquer en l'absence de la disposition inapplicable, et ce tout en respectant l'intention des parties.

Les intitulés portés en tête de chaque article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

9.16.4 Application et renonciation

Toute notification devant être donnée au titre de la présente politique sera censée avoir été donnée si elle est envoyée par lettre recommandée avec avis de réception ou par télécopie adressée au domicile élu comme indiqué en entête du contrat de service et sera censée avoir été reçue sept (7) jours après la date de cachet de la Poste dans le cadre de la lettre recommandée avec avis de réception et un (1) jour après la date d'envoi dans le cadre de la télécopie.

9.16.5 Force majeure

Dans un premier temps, les cas de force majeure suspendront l'exécution du contrat. Si les cas de force majeure ont une durée supérieure à celle indiquée dans le contrat, le contrat est résilié automatiquement, sauf accord contraire entre les parties. L'exécution des obligations reprendra son cours normal dès que l'évènement constitutif de la force majeure aura cessé.

L'AC ne saurait être tenue responsable et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'article 1148 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des cours et tribunaux français, des clauses contractuelles contenues dans la Déclaration des Pratiques associée et toutes autres conventions liant les parties (par exemple le contrat) :

Grève totale ou partielle, lock-out, émeute, trouble civil, insurrection, guerre civile ou étrangère, risque nucléaire, embargo, confiscation, capture ou destruction par toute autorité publique, intempérie, épidémie, blocage des moyens de transport ou d'approvisionnement pour quelque raison que ce soit, tremblement de terre, incendie, tempête, inondation, dégâts des eaux, restrictions gouvernementales ou légales, modifications légales ou réglementaires des formes de commercialisation, panne d'ordinateur, blocage des communications électroniques, y compris des réseaux de télécommunications, toute découverte scientifique majeure remettant en cause en totalité ou en partie les principes de la cryptographie asymétrique, toute conséquence d'une évolution technologique, non prévisible par l'AC, remettant en cause les normes et standards de sa profession et tout autre cas indépendants de la volonté des parties empêchant l'exécution normale du présent contrat.

9.17 AUTRES DISPOSITIONS

En vertu des articles 323-1 à 323-7 du Code pénal, applicable lorsqu'une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc.

Les peines encourues varient de 2 à 5 ans d'emprisonnement et d'une amende allant de 30.000 à 375.000 euros pour les personnes morales.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctifs, droits d'auteur (par exemple : logiciels, pages WEB, bases de données, textes originaux, ...) est sanctionnée par les articles L. 716-1 et suivants du Code de la propriété intellectuelle

10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 REGLEMENTATION

Renvoi	Document
[CNIL]	*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004*
[DIRSIG]	*Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.*
[LCEN]	*Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.*
[ORDONNANCE]	*Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*
[PSCO_QUALIF]	*Note d'application, Règlement eIDAS : critères d'évaluation de la conformité des prestataires de services de confiance qualifiés, version 1.2 du 05/07/2017.*
[QPSCe]	*Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation*
[DécretRGS]	*Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005.*
[SIG]	*Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.*
[RGPD]	*Règlement Européen UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*

10.2 DOCUMENTS TECHNIQUES

Renvoi	Document
[RGS]	*Référentiel Général de Sécurité - version 2.0.*
[PROFILS]	*Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques DT-FL-1310-002-PC-PROFILS*
[RGS_A1]	*RGS – Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques- Version 3.0.*
[RGS_A4]	*RGS – Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 3.0.*
[CWA14167-1]	*CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1*
[CWA14167-2]	*CWA 14167-2 (2003-10) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP). Ce PP a été certifié EAL4+.*
[CWA14167-3]	*CWA 14167-3 (2003-10) Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)*

[CWA14167-4]	*CWA 14167-4 (2003-10) Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO-PP). Ce PP a été certifié EAL4+.*
[CWA14169]	*CWA 14169 (2002-04) Secure Signature Creation Devices (SSCD). Ce PP a été certifié EAL4+.*
[EN_CP]	*EN 319 411-1 V1.3.1 (mai 2021) Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*
[EN_QCP]	*EN 319 411-2 V2.4.1 (novembre 2021) Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*
[PROG_ACCRED]	*COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – version publiée cf www.cofrac.fr*
[RFC2560]	*IETF - Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol, RFC 2560 - juin 1999*
[RFC3647]	*IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003*
[X.509]	*Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version mars 2000 (complete par les correctifs techniques n° 1 d'octobre 2001, n° 2 d'avril 2002 et n° 3 d'avril 2004)*
[PP_HORO]	*DCSSI - Profil de Protection - Systèmes d'horodatage EAL3+ DCSSI PP 2008/07*
[972-1]	*DCSSI - Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter – N° 972-1/SGDN/DCSSI du 17/07/2003*
[BRG]	*CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates - Version en vigueur.*
[EVCG]	*CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates - Version en vigueur.*
[SOGIC-CRYPTO]	*SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms - Version en vigueur.*

11 ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC

11.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR et, éventuellement, des réponses OCSP), ainsi que, le cas échéant, générer les bi-clés des certificats émis, doit répondre aux exigences de sécurité suivantes :

- si les bi-clés des certificats émis sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- si les bi-clés des certificats émis sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif cryptographique du bénéficiaire et assurer leur destruction sûre après ce transfert ;
- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

Le module cryptographique de l'AC détecte les tentatives d'altérations physiques et entre dans un état sûr quand une tentative d'altération est détectée.

11.2 EXIGENCES SUR LA QUALIFICATION

Le module cryptographique matériel utilisé pour la génération et la mise en œuvre des clés des AC est évalué selon les Critères Communs au niveau EAL 4+, et qualifié au niveau renforcé par l'ANSSI.

12 ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF CRYPTOGRAPHIQUE

12.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le dispositif cryptographique, utilisé par le bénéficiaire pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- si la bi-clé du certificat émis est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer un cachet ou une authentification qui ne peut être falsifiée sans la connaissance de la clé privée.

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques doivent être mises en place afin de :

- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de régénération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif ;
- Assurer pour le serveur légitime uniquement, d'une part, la fonction d'authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, et protéger la clé privée contre toute utilisation par des tiers ;
- Permettre de garantir l'authenticité et l'intégrité de la clé symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données.

12.2 EXIGENCES SUR LA QUALIFICATION

L'AC ne fournit pas le dispositif de protection des éléments secrets, il est recommandé d'utiliser un dispositif qualifié au niveau renforcé.